QA241
N6

The Library of

Brown
University

Niels Nielsen.

ELEMENTÆR TALTEORI

ELEMENTÆR
TALTEORI

EFTER FORELÆSNINGER HOLDTE
VED KØBENHAVNS UNIVERSITET

AF

DR. **NIELS NIELSEN**
PROFESSOR I MATEMATIK

GYLDENDALSKE BOGHANDEL
NORDISK FORLAG
KØBENHAVN OG KRISTIANIA
1912

QA241
N6

1,32
32727

TRYKT HOS J. JØRGENSEN & CO. (M. A. HANNOVER) KØBENHAVN

KAPITEL I.

Om division.

§ 1. Divisionsrester.

Vi forudsætter bekendt den af de hele tal dannede talmængde og de fire regningsarter anvendte paa denne talmængdes elementer.

For paa dette grundlag at fremstille grundtrækkene af den saakaldte elementære eller lavere talteori maa vi nødvendigvis begynde med at udvide læren om division paa følgende maade:

Opgives de to hele tal D og d, og vælges det tredje hele tal q vilkaarlig, bestemmer ligningen

$$D = dq + r \tag{1}$$

entydig det fjerde hele tal r; i (1) kaldes D dividenden, d modulus (divisor), q kvotienten og r resten. Da kvotienten kan være et hvilketsomhelst helt tal, bestemmer ligningen (1) for opgiven dividend og modulus uendelig mange divisionsrester.

Er m et hvilketsomhelst helt tal, og vælges kvotienten $q - m$, faas den med (1) analoge ligning

$$D = d(q - m) + r_1, \tag{2}$$

hvoraf ved sammenligning med (1)

$$r_1 = r + md, \tag{3}$$

og altsaa gælder sætningen:

I. *Alle de rester, som svarer til en given dividend og en given modulus, danner en differensrække med modulus til differens.*

Forudsættes d positiv, indeholder den ved (3) definerede restrække et og kun et led r', der tilfredsstiller betingelserne

$$0 \leqq r' \leqq d - 1; \tag{4}$$

denne ganske bestemte rest kaldes den til dividenden D og modulus d svarende *principale* divisionsrest.

Et hvilketsomhelst helt tal maa derfor modulo d have et ganske bestemt af de d hele tal

$$0,\ 1,\ 2,\ 3,\ \cdots\cdots,\ d-1 \tag{5}$$

til principal rest.

Restrækken (3) indeholder ligeledes et og kun et led r'', der tilfredsstiller betingelserne

$$-\frac{d}{2} < r'' \leqq \frac{d}{2}; \tag{6}$$

den saaledes bestemte rest r'' kaldes den til D og d hørende *numerisk mindste* rest; anvendes denne bestemte rest, skrives (1) hyppig paa formen

$$D = dq \pm \rho, \quad 0 \leqq \rho \leqq \tfrac{1}{2}d; \tag{7}$$

haves netop $\rho = \frac{1}{2}d$, idet d altsaa forudsættes lige, maa vi i (7) ikke tage ρ med negativt tegn.

I den almindelige lære om division haves et middel til at bestemme den til D og d svarende principale rest r'; derefter bestemmes den numerisk mindste rest r'' let. For $r' \leqq \frac{1}{2}d$ haves nemlig $r'' = r'$, medens man for $\frac{1}{2}d < r' \leqq d - 1$ finder $r'' = r' - d$.

Haves for den principale rest $r' = 0$, finder man ligeledes for den numerisk mindste rest $r'' = 0$, og ligningerne (1) og (7) antager formen

$$D = dq. \tag{8}$$

I dette tilfælde kaldes q den til dividenden D og modulus d hørende fuldstændige kvotient, divisionen siges at »gaa op«, og D er et multiplum af d, medens d kaldes en faktor eller en divisor i D.

I ligningen (8) kaldes endvidere d og q komplementære divisorer i D; antages $q > 1$, kaldes d en *alikvot* del af D. Tallet 1 er saaledes en alikvot del af ethvert helt tal større end 1.

Samtlige multipla af et helt tal d er altsaa af formen md, hvor m er et hvilketsomhelst helt tal; disse multipla af d danner derfor en differensrække med differensen d, og et af leddene i denne række er 0.

Med disse definitioner udledes af (1) den fundamentale sætning:

II. *Ethvert helt tal t, som gaar op i baade dividenden D og modulus d, gaar ligeledes op i ethvert af leddene i den til D og d hørende restrække.*

Haves nemlig $D = at$, $d = bt$, findes af (1) $r = t(a - bq)$, og altsaa erholdes for det almindelige led r_1 i restrækken (3) $r_1 = t(a - qb + mb)$.

Omvendt haves:

III. *Ethvert helt tal t, som gaar op i modulus d og en vilkaarlig rest r, gaar ligeledes op i dividenden D og derfor i ethvert af restrækkens led.*

Antages $d = at$, $r = bt$, faas af (1) $D = (aq + b)t$, og ved anvendelse af (3) $r_1 = (b + ma)t$.

Er endvidere t et vilkaarligt helt tal, findes ved (1) og (3)

$$tD = td \cdot q + tr, \quad r_1 = t(r + md), \tag{9}$$

hvoraf sætningen:

IV. *Multipliceres dividenden D og modulus d med et helt tal t, vil ethvert af restrækkens led ligeledes blive multipliceret med t.*

Da man omvendt af (9) kan udlede (1) og (3) ved at dividere med t, faas den til IV svarende omvendte sætning:

V. *Divideres dividenden D og modulus d med et helt tal t, som gaar op i dem begge, vil ethvert af restrækkens led ligeledes blive divideret med t.*

Betegner i (1) r den principale eller den numerisk mindste rest, og er t positiv, vil i den første ligning (9) tr ligeledes være henholdsvis den principale eller den numerisk mindste rest, og omvendt.

Haves de to ligninger

$$D = dq + r, \quad D_1 = dq_1 + r_1, \tag{10}$$

findes umiddelbart

$$\begin{cases} D \pm D_1 = d(q \pm q_1) + (r \pm r_1) \\ DD_1 = d(dqq_1 + qr_1 + q_1 r) + rr_1, \end{cases} \tag{11}$$

hvoraf følgende almindelige sætning uden vanskelighed udledes:

VI. *Er i den hele rationale funktion af n variable*

$$F(x_1, x_2, x_3, \cdots, x_n) = \Sigma a_{p_1, p_2, p_3, \ldots, p_n} x_1^{p_1} x_2^{p_2} x_3^{p_3} \cdots x_n^{p_n} \tag{12}$$

samtlige koefficienter og variable hele tal, kan man finde resten af F for en vilkaarlig modulus d ved for hver enkelt koefficient og variabel at sætte dens til modulus d svarende principale rest.

Læren om de principale rester spiller en vigtig rolle i den elementære talteori. Læseren kan overbevise sig om rigtigheden af denne bemærkning ved at anvende de i følgende eksempler angivne resultater paa nedenstaaende opgaver 1—4:

Eks. 1. Kvadratet paa et ulige tal giver altid modulo 8 den principale rest 1.

Man finder nemlig

$$(2n + 1)^2 = 4n(n + 1) + 1 = 8m + 1; \tag{13}$$

ti $n(n + 1)$ er altid et lige tal.

Eks. 2. Alle kvadrattal maa modulo 4 enten give den principale rest 0 eller 1.

Eks. 3. Alle kvadrattal maa modulo 3 enten give den principale rest 0 eller 1.

Man finder nemlig for alle hele værdier af n

$$(3n)^2 = 9n^2, \quad (3n + 1)^2 = 3(3n^2 + 2n) + 1,$$
$$(3n + 2)^2 = 3(3n^2 + 4n + 1) + 1.$$

To hele tal siges at være af samme eller af modsat paritet, eftersom deres principale rester modulo 2 er ligestore eller forskellige.

Vis, at samtlige Kubiktal modulo 7 kun kan give resterne $-1, 0, +1$, og angiv hvilke Kubiktal, der giver hver enkelt af disse rester.

1. Vis, at et tal af formen $4n + 3$ hverken kan være et kvadrattal eller en sum af to kvadrattal.
2. Vis, at et tal af formen $8n + 7$ hverken kan være et kvadrattal eller en sum af to eller en sum af tre kvadrattal.
3. Hvis tallene a, b og c alle modulo 4 giver den principale rest 1, kan ligningen

$$ax^2 + by^2 + cz^2 = 0$$

ikke tilfredsstilles af andre hele værdier for x, y og z end $x = y = z = 0$.

Eks. $a = b = 1$, $c = -3$.

4. Vis, at ligningen

$$3x^2 - y^2 = 1$$

ikke tilfredsstilles af hele værdier for x og y.

5. Antages $p > 1$ og hel, skal man finde, for hvilke positive hele m tallet $p^m + 1$ er deleligt med $p^2 + 1$.

§ 2. Den Euklidiske algoritme.

Vi tænker os modulus d og dividenden D positive; hvis den tilsvarende principale rest $r < d$ ikke er 0, kan vi tage r til modulus og d til dividend og derved finde den ny principale rest $r_1 < r$.

Er r_1 heller ikke nul, kan vi atter vælge r_1 til modulus r til dividend og derved finde den ny principale rest $r_2 < r_1$ o. s. v.

Paa denne maade kan vi imidlertid ikke fortsætte ubegrænset; thi ved hver gentagelse af operationen faas stedse en principal rest, der er mindre end den foregaaende; vi maa derfor efter et vist antal divisioner faa den principale rest 0.

Svarende til de positive hele tal D og d faar vi derfor følgende kæde af ligninger, som vi vil kalde den til D og d hørende *Euklidiske* algoritme:

$$(1)\qquad \begin{cases} D = dq + r, & 0 < r < d, \\ d = rq_1 + r_1, & 0 < r_1 < r, \\ r = r_1 q_2 + r_2, & 0 < r_2 < r_1, \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ r_{n-2} = r_{n-1} q_n + r_n, & 0 < r_n < r_{n-1}, \\ r_{n-1} = r_n q_{n+1}. \end{cases}$$

Anvendes de numerisk mindste rester istedetfor de principale, faas følgende anden form for den *Euklidiske* algoritme:

$$(2)\qquad \begin{cases} D = dq' \pm r', & 0 < r' \leqq \tfrac{1}{2} d, \\ d = r'q'_1 \pm r'_1, & 0 < r'_1 \leqq \tfrac{1}{2} r', \\ r' = r'_1 q'_2 \pm r'_2, & 0 < r'_2 \leqq \tfrac{1}{2} r_1' \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ r'_{m-2} = r'_{m-1} q'_m \pm r'_m, & 0 < r'_m \leqq \tfrac{1}{2} r'_{m-1}. \\ r'_{m-1} = r'_m q'_{m+1}. \end{cases}$$

Eks. Til tallene $D = 315$, $d = 195$ faas de til (1) og (2) svarende algoritmer: $315 = 195 \cdot 1 + 120$, $195 = 120 \cdot 1 + 75$, $120 = 75 \cdot 1 + 45$, $75 = 45 \cdot 1 + 30$, $45 = 30 \cdot 1 + 15$, $30 = 15 \cdot 2$; $315 = 195 \cdot 2 - 75$, $195 = 75 \cdot 3 - 30$, $75 = 30 \cdot 2 + 15$, $30 = 15 \cdot 2$.

Anvendes § 1, III paa algoritmerne (1) og (2), ser man, at r_n og r'_m begge maa gaa op i baade d og D, medens § 1, II viser, at ethvert tal t, der gaar op i baade D og d, tillige maa gaa op i r_n og r'_m, og altsaa faas sætningen:

I. *De sidste divisorer r_n og r'_m i (1) og (2) er de største positive hele tal, som gaar op i baade D og d, og altsaa haves*

$$(3)\qquad r_n = r'_m.$$

---

6. Idet a, n og p er positive hele tal, skal man danne den til tallene $a^n - 1$ og $a^p - 1$ svarende *Euklidiske* algoritme.

§ 3. Største fælles faktor og mindste fælles multiplum.

Største fælles faktor for en samling hele tal er det største positive hele tal, der gaar op i dem alle. Drejer det sig kun om de to hele tal D og d, haves ifølge § 2, I:

I. *Største fælles faktor for D og d er den sidst brugte divisor i de til D og d svarende Euklidiske algoritmer.*

To tal kaldes indbyrdes primiske, naar deres største fælles faktor er 1.

Er f største fælles faktor for D og d, faas sætningerne:

II. *Ethvert helt tal, som gaar op i baade D og d, gaar ligeledes op i f.*

III. *Største fælles faktor for mD og md er mf.*

IV. *Er m en fælles divisor i D og d, har $D:m$ og $d:m$ største fælles faktor $f:m$.*

V. *Tallene $D:f$ og $d:f$ er indbyrdes primiske.*

Største fælles faktor for de n hele tal $D_1, D_2, D_3, \cdots, D_n$ kan ifølge II bestemmes, idet man finder største fælles faktor f_1 for D_1 og D_2, dernæst største fælles faktor f_2 for f_1 og D_3, o. s. v.

Af ovenstaaende sætninger findes endvidere følgende:

VI. *Hvis t er primisk med a og gaar op i produktet ab, saa gaar t op i b.*

Da t og a har største fælles faktor 1, har tb og ab ifølge III største fælles faktor b, og ifølge II maa t derfor gaa op i b.

VII. *Er den uforkortelige Brøk $a:b$ lig med brøken $c:d$, maa c og d være samme multiplum af henholdsvis a og b.*

Af $a:b = c:d$ finder man $ad = cb$; da a her er primisk med b, maa a gaa op i c; sættes $c = ma$, faas $d = mb$.

VIII. *Gaar to indbyrdes primiske tal a og b hver for sig op i et tredje tal c, gaar produktet ab ligeledes op i c.*

Sættes $c = ma$, gaar b ifølge VI op i m; sættes $m = m_1 b$, faas $c = m_1 ab$.

Ved hjælp af VIII kan man let bestemme den fælles form for et tal A, hvori to givne tal a og b begge gaar op; A kaldes i dette tilfælde et fælles multiplum for a og b.

Har de to givne tal a og b største fælles faktor f, og sættes $a = a_1 f$, $b = b_1 f$, er a_1 og b_1 indbyrdes primiske.

Ethvert tal A, hvori baade a og b gaar op, maa altsaa ifølge VIII være af formen

$$A = a_1 b_1 f m, \tag{1}$$

hvor m er et helt tal.

Ved mindste fælles multiplum for to hele tal forstaas det mindste positive hele tal, hvori begge de givne gaar op.

Er med de foregaaende betegnelser M mindste fælles multiplum for de to givne tal a og b, findes derfor ifølge (1) $m = 1$, og altsaa er

(2) $$M = a_1 b_1 f, \quad A = mM,$$

hvoraf

$$Mf = a_1 f \cdot b_1 f = ab,$$

og dermed har vi bevist sætningen:

IX. *Produktet af to tal er lig med produktet af disse tals største fælles faktor og mindste fælles multiplum.*

Mindste fælles multiplum for en samling hele tal er det mindste positive hele tal, hvori de alle gaar op.

Mindste fælles multiplum for tallene $a_1, a_2, a_3, \cdots, a_n$ kan findes, idet man først bestemmer mindste fælles multiplum M_1 for a_1 og a_2, dernæst mindste fælles multiplum M_2 for M_1 og a_3, o. s. v.

---

7. Find, med betegnelserne i § 2, (1) og (2), største fælles faktor for r_p og r_{p+1} og for r'_q og r'_{q+1}.
8. Angiv den nødvendige og tilstrækkelige betingelse for, at en sum af to uforkortelige brøker kan være et helt tal.
9. Bestem det mindste positive hele tal m, for hvilket $a^n - 1$ og $a^p - 1$ begge gaar op i $a^m - 1$; a, n og p er positive hele tal.
10. Vis, at de tre tal i hver af de følgende fire grupper

$$3n+1,\ 2n+1,\ 12n+5; \qquad 2n+1,\ 3n+2,\ 12n+7;$$
$$2n+2,\ 4n+3,\ 6n+5; \qquad n+1,\ 6n+5,\ 12n+11$$

to og to er indbyrdes primiske; n antages positiv hel.

11. Antages n og m positive hele, og sættes

$$B_n = x^n + 1, \quad A_n = 1 + x + x^2 + \cdots + x^{n-1} + x^n,$$

skal man finde største fælles faktor for B_m og A_n samt for A_n og A_2.

§ 4. Ubestemte ligninger af første grad med to ubekendte.

Antages a_1, a_2 og b at være tre givne rationale tal, vil vi søge de hele værdier af x_1 og x_2, som tilfredsstiller ligningen

$$a_1 x_2 + a_2 x_1 = b. \tag{1}$$

Ved løsningen af denne opgave kan vi aabenbart antage, at de tre givne rationale tal a_1, a_2 og b alle er hele; ti var dette ikke tilfældet, kunde vi multiplicere med mindste fælles multiplum for de indgaaende nævnere.

Vi kan endvidere antage, at der ikke eksisterer noget helt tal, forskelligt fra 1, som gaar op i baade a_1, a_2 og b; ti et saadant helt tal kunde bortdivideres.

Endelig kan a_1 og a_2 begge antages positive; var nemlig f. eks. a_1 negativ, multiplicerede vi (1) med -1, og blev derved a_2 negativ, sætter vi $x_2 = -x'_2$.

Efter disse bemærkninger vil vi nu bevise den almindelige sætning:

I. *Den nødvendige og tilstrækkelige betingelse for, at ligningen* (1), *hvor de givne koefficienter* a_1, a_2 *og* b *tilfredsstiller alle de lige nævnte betingelser, giver hele løsninger for* x_1 *og* x_2, *er, at* a_1 *og* a_2 *er indbyrdes primiske.*

Det er indlysende, at ovennævnte betingelse er nødvendig; ti havde a_1 og a_2 en fælles faktor $f > 1$, og var x_1 og x_2 hele tal, maatte f gaa op i venstre side af (1) og dog være primisk med b, hvilket er umuligt.

For at vise, at ovennævnte nødvendige betingelse ogsaa er tilstrækkelig, antager vi $a_1 > a_2$ og danner den til a_1 og a_2 svarende *Euklidiske* algoritme

$$\begin{aligned}
a_1 &= a_2 q_2 + a_3 \\
a_2 &= a_3 q_3 + a_4 \\
&\cdots\cdots\cdots\cdots\cdots \\
a_{n-2} &= a_{n-1} q_{n-1} + a_n \\
a_{n-1} &= a_n q_n;
\end{aligned}$$

da a_1 og a_2 er indbyrdes primiske, findes $a_n = 1$.

Sættes nu med de saaledes bestemte ufuldstændige kvotienter $q_2, q_3, \ldots, q_{n-1}$:

$$(2)\qquad \begin{cases} x_1 = -x_2 q_2 + x_3 \\ x_2 = -x_3 q_3 + x_4 \\ x_3 = -x_4 q_4 + x_5 \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ x_{n-2} = -x_{n-1} q_{n-1} + x_n, \end{cases}$$

faas ved induktion af (1) almindelig

$$(3)\qquad a_r x_{r+1} + a_{r+1} x_r = b,$$

hvoraf for $r = n - 1$, idet $a_n = 1$:

$$a_{n-1} x_n + x_{n-1} = b,$$

og denne ligning er aabenbart tilfredsstillet af de to hele tal

$$(4)\qquad x_n = 0, \quad x_{n-1} = b,$$

hvorefter $x_{n-2}, x_{n-3}, \ldots, x_2, x_1$ findes ved hjælp af formlerne (2).

Efter at vi saaledes har bevist I, har vi endnu tilbage at bevise følgende sætning om (1):

II. *Er* $x_1 = \alpha$, $x_2 = \beta$ *et vilkaarligt sæt hele værdier af* x_1 *og* x_2, *som tilfredsstiller* (1), *bliver alle hele løsninger af denne ligning*

$$(5)\qquad x_1 = \alpha + m a_1, \quad x_2 = \beta - m a_2,$$

hvor m *er et hvilketsomhelst helt tal.*

Da

$$(6)\qquad a_1 \beta + a_2 \alpha = b,$$

er det indlysende, at alle de ved (5) bestemte hele tal tilfredsstiller (1).

Ved subtraktion af (1) og (6) faas

$$a_1 (x_2 - \beta) = -a_2 (x_1 - \alpha),$$

hvoraf, idet a_1 og a_2 er indbyrdes primiske,

$$x_1 - \alpha = m a_1, \quad x_2 - \beta = -m a_2,$$

hvor m er et vilkaarligt helt tal.

Metoden, den første systematiske der kendes, skyldes Rolle; den er fremsat i hans Traité d'algèbre; Paris 1690, det samme skrift, der indeholder hans berømte algebraiske sætning.

Af (5) slutter man, at samtlige værdier af x_1 og x_2 danner differensrækker med differenserne a_1 og a_2.

---

12. Idet a, b og c er positive hele og to og to indbyrdes primiske, skal man vise, at de positive hele tal x og y, hvor $x < b$ og $y < c$, entydig kan bestemmes ved ligningen

$$\frac{a}{bc} = \frac{x}{b} + \frac{y}{c} + k,$$

hvor k er et helt tal.

13. Udvid sætningen i foranstaaende opgave, naar den givne uforkortelige brøks nævner er et produkt af n faktorer, der to og to er indbyrdes primiske.

§ 5. **Kongruenser.**

To tal a og b, der for en vis modulus d har den samme restrække, kaldes efter *Gauss*[1]) kongruente modulo d; dette betegnes

(1) $$a \equiv b \pmod{d}.$$

Da a og b modulo d skal have den samme restrække, er det muligt at vælge to hele tal q og q_1, saaledes at

$$a = dq + r, \quad b = dq_1 + r, \quad a - b = d(q - q_1),$$

hvoraf sætningen:

I. *Den nødvendige og tilstrækkelige betingelse for, at kongruensen* (1) *er rigtig, er, at* $a - b$ *er delelig med modulus* d.

Kongruenser for samme modulus kan i mange henseender behandles paa samme maade som ligninger.

Haves nemlig foruden (1) kongruensen

(2) $$a_1 \equiv b_1 \pmod{d},$$

faas ved anvendelse af I og formlerne § 1, (11)

---

[1]) Disquisitiones arithmeticæ, art. 1; 1801. Untersuchungen über höhere Arithmetik, p. 1; Berlin 1889. Werke, Bd. I, p. 9.

(3) $$a \pm a_1 \equiv b \pm b_1 \pmod{d}$$

(4) $$aa_1 \equiv bb_1 \pmod{d},$$

og, idet n er positiv hel,

(5) $$a^n \equiv a_1^n \pmod{d}.$$

Haves i (3) og (4) $a_1 = b_1$, ser man, at man i en kongruens tør addere eller subtrahere samme hele tal til de to led, og at disse to led tør multipliceres med samme hele tal.

Af kongruenserne

$$a + b \equiv c \pmod{d}, \quad -b \equiv -b \pmod{d}$$

findes specielt

$$a \equiv c - b \pmod{d};$$

et led tør altsaa flyttes fra den ene side af kongruenstegnet til den anden, naar blot dets fortegn ændres.

Af kongruensen

(6) $$ac \equiv bc \pmod{d}$$

tør man imidlertid almindeligvis ikke bortdividere c.

Af kongruenserne

$$18 \equiv 81 \pmod{9}, \quad 15 \equiv 20 \pmod{5}$$

tør man saaledes ikke bortdividere henholdsvis 3 og 5.

Da (6) er ensbetydende med, at d gaar op i $ac - bc = c(a - b)$, faas ifølge § 3, VI:

II. *En fælles faktor for de to led i en kongruens kan altid bortdivideres, naar den blot er primisk med modulus.*

Til kvotienten $b : a$ svarer i læren om kongruenser tallet x, der defineres ved kongruensen

(7) $$ax \equiv b \pmod{d};$$

da denne kongruens er ensbetydende med, at d gaar op i $ax - b$, altsaa med den ubestemte ligning

$$ax + dy = b,$$

ser man ifølge § 4, I, at (7) altid definerer hele x, naar blot a og d er indbyrdes primiske. Kan denne ubestemte ligning

løses, faar man uendelig mange værdier for x; disse værdier danner altid en differensrække.

Om kongruensen (7) vil vi endnu her bevise sætningen:

III. *Er i kongruensen* (7) *a primisk med d, og er modulus d produktet af de alikvote dele* d_1 *og* d_2, *kan denne kongruens erstattes af to andre, hvis moduler er henholdsvis* d_1 *og* d_2.

Betragtes nemlig først kongruensen

$$ax \equiv b \pmod{d_1}, \tag{8}$$

kan denne løses, fordi a og d_1 er indbyrdes primiske; man finder

$$x = x_1 + d_1 y, \tag{9}$$

hvor y er et vilkaarligt helt tal, og der eksisterer følgelig et helt tal c, saaledes at

$$ax_1 - b = -d_1 c; \tag{10}$$

derved erholdes

$$ax - b = ax_1 - b + ad_1 y = d_1 (ay - c).$$

Kongruensen (7) vil derfor aabenbart være tilfredsstillet, naar det i (9) forekommende vilkaarlige tal y bestemmes saaledes, at

$$ay \equiv c \pmod{d_2}. \tag{11}$$

Finder man ved (11)

$$y = y_1 + md_2,$$

erholdes ved (9) den fuldstændige løsning af (7) paa formen

$$x = x_1 + d_1 y_1 + md. \tag{12}$$

Eks. 1. For at løse kongruensen

$$7x \equiv 2 \pmod{9}, \tag{13}$$

betragter vi først

$$7x \equiv 2 \pmod{3}, \quad x = 2 + 3y,$$

og altsaa erholdes

$12 + 21y \equiv 0 \pmod 9$, $4 + 7y \equiv 0 \pmod 3$, $y = 2 + 3p$,

og den almindelige løsning af (13) bliver

$$x = 8 + 9p.$$

Eks. 2. For at finde x af

(14) $$13x \equiv 7 \pmod{15}$$

sætter vi

$$13x \equiv 7 \pmod 3, \quad x = 1 + 3y,$$

og vi finder derefter

$6 + 39y \equiv 0 \pmod{15}$, $2 + 13y \equiv 0 \pmod 5$, $y = 1 + 5p$,

og altsaa bliver løsningen af (14)

$$x = 4 + 15p.$$

Vi skal senere, i § 36, omtale en interessant anvendelse af III.

---

14. Idet p er et ulige tal, som er primisk med a, skal kongruensen

$$ax^2 + bx + c \equiv 0 \pmod p$$

reduceres til en anden af formen

$$y^2 + A \equiv 0 \pmod p.$$

15. Reducer kongruensen

$$17x^2 + 14x + 3 \equiv 0 \pmod{15}.$$

§ 6. **Talsystemer.**

Betegner p et vilkaarligt helt tal, større end 1, kan ethvert positivt helt tal $n \geqq p$ bringes paa formen

(1) $$n = a_r p^r + a_{r-1} p^{r-1} + \cdots + a_1 p + a_0,$$

hvor koefficienterne a_s tilfredsstiller betingelserne

(2) $0 \leqq a_s \leqq p - 1$, $s = 0, 1, 2, \ldots, r-1$; $0 < a_r \leqq p - 1$.

Koefficienterne a_s kan nemlig efterhaanden bestemmes som principale rester ved følgende divisioner

$$\begin{aligned}
n &= pn_1 + a_0, & 0 \leqq a_0 &\leqq p-1\\
n_1 &= pn_2 + a_1, & 0 \leqq a_1 &\leqq p-1\\
n_2 &= pn_3 + a_2, & 0 \leqq a_2 &\leqq p-1\\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\
n_{r-1} &= pn_r + a_{r-1}, & 0 \leqq a_{r-1} &\leqq p-1\\
n_r &= p\cdot 0 + a_r, & 0 < a_r &\leqq p-1.
\end{aligned}$$

Skrives tallet n paa formen (1), hvilket altsaa kun er muligt paa en maade, siges n at være et $(r+1)$-cifret tal i p-talsystemet, og de $r+1$ koefficienter a_s kaldes dette tals cifre, medens p er systemets basis. Summen af cifrene kaldes tværsummen af n; betegnes denne tværsum ved $t_p(n)$, haves altsaa

$$t_p(n) = a_0 + a_1 + a_2 + \cdots + a_r. \tag{3}$$

Det størst mulige $(r+1)$-cifrede tal i p-talsystemet er aabenbart

$$(p-1)(p^r + p^{r-1} + \cdots + p + 1) = p^{r+1} - 1. \tag{4}$$

Er d_1 og d_2 komplementære divisorer i $p-1$, altsaa $p-1 = d_1 d_2$, findes

$$p = d_1 d_2 + 1 = (p-1) + 1, \quad p \equiv 1 \pmod{d_1};$$

ved anvendelse af § 1, VI faas derved sætningen:

I. *Skrives n i p-talsystemet, og er d en vilkaarlig divisor i* $p-1$, *haves*

$$n \equiv t_p(n) \pmod{d}. \tag{4}$$

Betegner d_1 og d_2 komplementære divisorer i $p+1$, er altsaa $p+1 = d_1 d_2$, findes

$$p = d_1 d_2 - 1 = (p+1) - 1, \quad p \equiv -1 \pmod{d_1},$$

og altsaa erholdes den ny sætning:

II. *Er d en vilkaarlig divisor i* $p+1$, *findes for det i* (1) *fremstillede tal n*:

$$n \equiv a_0 - a_1 + a_2 - a_3 + \cdots + (-1)^r a_r \pmod{d}. \tag{5}$$

Skrives tallene a, b og $a+b$ alle i p-talsystemet, haves ifølge (4)

$$t_p(a)+t_p(b)\equiv t_p(a+b)\equiv a+b \pmod{(p-1)}, \tag{6}$$

og altsaa finder man

$$t_p(a)+t_p(b)-t_p(a+b)=d(p-1), \tag{7}$$

hvor d er et helt tal, der aldrig kan være negativt; altsaa haves $d\geqq 0$.

Tallene a og b kan nemlig begge skrives paa formen

$$\begin{cases} a=a_r p^r+a_{r-1}p^{r-1}+\cdots+a_s p^s+\cdots+a_1 p+a_0 \\ b=b_r p^r+b_{r-1}p^{r-1}+\cdots+b_s p^s+\cdots+b_1 p+b_0, \end{cases} \tag{8}$$

hvor i en af fremstillingerne nogle af de højeste potenser af p kan falde bort, idet de tilsvarende koefficienter er 0.

Haves nu i (8) bestandig

$$a_s+b_s\leqq p-1, \quad 0\leqq s\leqq r,$$

faas aabenbart i (7) $d=0$. Er derimod

$$a_s+b_s=p+d_s, \quad 0\leqq d_s\leqq p-2, \tag{9}$$

bliver i $a+b$ koefficienten til p^s lig med d_s, medens p^{s+1} faar koefficienten $a_{s+1}+b_{s+1}+1$, der muligvis atter maa reduceres ved en formel analog med (9), o. s. v.

I dette tilfælde faas derfor i (7) $d\geqq 1$.

---

16. Undersøg de til samme tal n svarende tværsummer $t_2(n)$ og $t_4(n)$.

17. Vis, at ligningen

$$1+x+x^2+x^3+x^4=y^2$$

ikke har andre positive hele løsninger i x og y end $x=3$, $y=11$. Tallet 11111 er saaledes kun et kvadrattal i et eneste talsystem, nemlig det med basis 3.

Løsning til 17. Da $x=1$ giver $y=5$, kan vi indskrænke os til at betragte $x>1$; skrives da y i x-talsystemet, haves $y=\alpha x^2+\alpha x+\beta$. I udtrykket for y^2 faar x^3-koefficienten $2\alpha\beta$, saaledes at $\alpha=0$, og det kommer da an paa at løse ligningen

$$x^3+x^2+x+1=2\alpha\beta x^2+\beta^2,$$

der kun er mulig, naar

$$2\alpha\beta=x+1, \quad \beta^2=x+1,$$

hvilket giver $\beta=2$, $x=3$, og derefter findes $y=11$.

KAPITEL II.

Primtal.

§ 7. Sætninger om primtal.

Et primtal er et helt tal større end 1, som kun er deleligt med 1 og sig selv.

To forskellige primtal er derfor altid indbyrdes primiske, og et primtal er primisk med ethvert helt tal, hvori det ikke gaar op.

Af de i § 3 beviste sætninger udledes her specielt:

I. *Den nødvendige og tilstrækkelige betingelse for, at et primtal gaar op i et produkt, er, at det gaar op i mindst en af faktorerne.*

At denne betingelse er tilstrækkelig, ses umiddelbart; gaar nu primtallet p op i ab, og gaar p ikke op i a, er p og a indbyrdes primiske, og p maa altsaa ifølge § 3, VI gaa op i b.

Af I faas specielt:

II. *Den nødvendige og tilstrækkelige betingelse for, at et primtal gaar op i en potens, er, at det gaar op i roden.*

III. *Er tallene a og b indbyrdes primiske, er vilkaarlige potenser af disse tal, a^m og b^n, ligeledes indbyrdes primiske.*

Var nemlig a^m og b^n ikke indbyrdes primiske, maatte et primtal gaa op i begge disse potenser; men ifølge II maatte dette primtal da ligeledes gaa op i baade a og b, og det er umuligt.

Af III faas specielt:

IV. *Enhver potens af en uforkortelig brøk er paany en uforkortelig brøk.*

Af IV i forbindelse med § 3, VII faas endvidere:

V. *Ligningen*

$$x^n = \frac{a}{b}, \tag{1}$$

hvor $a:b$ er en uforkortelig brøk, tilfredsstilles da og kun da af et rationalt x, naar a og b hver for sig er n^{te} potenser af hele tal.

Skal nemlig (1) tilfredsstilles af den uforkortelige brøk $x = p : q$, haves

$$\frac{p^n}{q^n} = \frac{a}{b}, \tag{2}$$

og da begge disse brøker er uforkortelige, er (2) da og kun da mulig, naar $a = p^n$ og samtidig $b = q^n$.

Ethvert helt tal større end 1, som ikke er et primtal, kaldes et sammensat tal; et sammensat tal kan derfor altid paa mindst en maade skrives som et produkt af to faktorer, der begge er større end 1.

Et sammensat tal siges at være opløst i primfaktorer, naar det er skrevet som et produkt af lutter primtal. Om denne fremstillingsform haves sætningen:

VI. *Et sammensat tal kan paa en og kun paa en maade opløses i primfaktorer.*

Betyder $p_1, p_2, p_3, \ldots, p_n$ forskellige primtal, og haves

$$p_1^{a_1} p_2^{a_2} \ldots p_r^{a_r} = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}, \tag{3}$$

hvor $a_1 \neq \alpha_1$, kan vi antage, at $a_1 > \alpha_1$; ved bortdivision af $p_1^{\alpha_1}$ findes derfor af (2)

$$p_1^{a_1-\alpha_1} p_2^{a_2} \ldots p_r^{a_r} = p_2^{\alpha_2} \ldots p_r^{\alpha_r},$$

hvilket er umuligt, fordi venstre side er delelig med p_1, højre derimod ikke. Ligningen (3) er derfor da og kun da rigtig, naar

$$\alpha_1 = a_1, \ \alpha_2 = a_2, \ \ldots, \ \alpha_r = a_r.$$

Skal et sammensat tal n opløses i primfaktorer, kan dette i almindelighed kun ske ved, at man prøver, hvilke primtal der gaar op i n og, tillige hvormange gange enhver saadan primtaldivisor gaar op i n. Findes paa denne maade

$$n = p_1^{a_1} p_2^{a_2} \ldots p_r^{a_r}, \tag{4}$$

siger man, at tallet n indeholder primfaktorerne $p_1, p_2, \ldots, p_r$ henholdsvis $a_1, a_2, \ldots, a_r$ gange.

18. Vis, at et tal af formen $4n + 3$ altid maa indeholde et ulige antal primfaktorer af denne form i ulige potenser.
19. Vis, at tre hele indbyrdes primiske tal aldrig kan være led i samme kvotientrække.
20. Vis, at tal af formen $a^p - 1$ aldrig kan være primtal for $a > 2$ og $p > 1$.
21. Vis, at $a^3 + (a + 2)^3$ altid er delelig med 4, og at kvotienten da og kun da er et primtal, naar $a = 1$.
22. Hvis m er positiv hel og ikke delelig med primtallet p, gaar $2^p - 1$ op i

$$1 + 2^m + 2^{2m} + \cdots + 2^{(p-1)m}.$$

23. Vis ved anvendelse af opg. 10, at ligningen

$$x(x + 1)(2x + 1) = 6y^2,$$

som aabenbart tilfredsstilles af $x = 1$, $y = 1$ og $x = 24$, $y = 70$, kun kan løses i hele tal, naar enten $x = 6n + 1$ eller $x = 6n$ [1]).

24. Vis, at den nødvendige og tilstrækkelige betingelse for, at kongruensen

$$x^2 + ay^2 \equiv 0 \pmod{p},$$

hvor p ikke gaar op i a, kan løses i hele indbyrdes primiske tal for x og y, er, at

$$u^2 + a \equiv 0 \pmod{p}$$

giver hele løsninger for u.

§ 8. **Om mængden af primtal. Faktortavler.**

Allerede *Euklid* beviste sætningen:

I. *Den af primtallene dannede talmængde er uendelig.*

Var der nemlig i hele talrækken kun de n primtal

[1]) Ovennævnte værdier $x = 1$, $y = 1$ og $x = 24$, $y = 70$ er de eneste værdisæt af positive hele tal, som tilfredsstiller den omtalte ligning; se *Th. Pepin* i Atti della Accademia Pontificia dei Nuovi Lincei, Bd. 35, p. 281—302; 1879. Tidligere beviser er enten unøjagtige (*Lucas* i Nouvelles Annales (2) Bd. 16, p. 429—431; 1877) eller mangelfulde (*Moret-Blanc* i Nouvelles Annales (2) Bd. 15, p. 46—48; 1876).

(1) $$p_1, p_2, \cdots, p_n,$$

maatte ethvert andet helt tal være deleligt med mindst et af disse primtal; men tallet

(2) $$p_1 p_2 p_3 \cdots p_n + 1$$

har ikke denne egenskab, og altsaa maa mængden af primtal være uendelig.

Betegner (1) de n første primtal ordnede efter størrelse, og dannes for de forskellige værdier af n de til (2) svarende tal, kan disse tal derfor kun være delelige med primtal større end p_n.

For de 5 første værdier af n findes primtallene

$$2+1=3,\ 2\cdot 3+1=7,\ 2\cdot 3\cdot 5+1=31,\ 2\cdot 3\cdot 5\cdot 7+1=211,$$
$$2\cdot 3\cdot 5\cdot 7\cdot 11+1=2311;$$

derimod findes for det sjette af disse tal [1])

$$2\cdot 3\cdot 5\cdot 7\cdot 11\cdot 13+1=30031=59\cdot 509.$$

Da man endnu ikke kender nogen simpel lov for antallet af de primtal, der er beliggende mellem to givne tal, maa man enten ved beregning af analytiske udtryk eller ved direkte optælling bestemme saadanne antal.

Den første af disse veje er fulgt af *Meissel* [2]), efter hvem antallet af primtal mindre end en milliard (1000 000 000) er

50 847 478.

Direkte optælling af mængden af de primtal, som er mindre end et vilkaarligt forud opgivet tal, kan ske ved hjælp af de saakaldte faktortavler, der angiver den mindste primfaktor (større end 5), som gaar op i de sammensatte tal.

Den første tavle af denne art (gaaende til 400 000) skyldes *Vega* [3]), den næste (gaaende til 1020 000) skyldes *Chernac* [4]).

[1]) *Legendre:* Théorie des nombres, Bd. I, p. 14; Paris 1830 (3. udg.). Zahlentheorie, Bd. I, p. 15; Leipzig 1893 (2. udg.).

[2]) Mathematische Annalen, Bd. 2, p. 636—642; 1872. Bd. 3, p. 523—525; 1872. Bd. 21, p. 304; 1883. Bd. 25, p. 251—257; 1885.

[3]) Tabulæ logarihmico-trigonometricæ; Leipzig 1797.

[4]) Cribrum arithmeticum. Deventer 1811.

Faktortavler af større udstrækning er beregnede af *Burckhardt*[1]), *Dase*[2]) og *James Glaisher*[3]). Korrektioner til disse faktortavler er givne af *N. P. Bertelsen*[4]).

I de sidste aar har *D. N. Lehmer*[5]) givet en faktortavle for de første 10 millioner. Akademiet i Wien besidder et endnu utrykt kæmpemanuskript af *J. P. Kulik* angivende den mindste divisor for alle sammensatte tal fra den 3dje til den 100de million.

Lehmer har imidlertid eftervist 226 fejl hos *Kulik*, alene for den 10de millions vedkommende.

Primtallenes fordeling i talrækken synes at være i høj grad uregelmæssig; man kender lange perioder af paa hinanden følgende ulige tal, der alle er sammensatte; saa langt undersøgelserne gaar, finder man paa den anden side par af paa hinanden følgende ulige tal, som begge er primtal.

Saaledes er f. eks. følgende samlinger af ulige tal alle sammensatte[6]):

$$115—125, \quad 1131—1149, \quad 1329—1359.$$

J. W. L. Glaisher[7]) giver forskellige sammenstillinger af denne art; af samme forfatter[8]) haves ligeledes samlinger af talpar $2n \pm 1$, der begge er primtal.

Betegner m et vilkaarlig stort helt tal, ved vi, at der eksisterer uendelig mange primtal større end m; men vi er ikke istand til at angive formen for et eneste saadant primtal.

Som et kuriosum bemærker vi, at (for hele x)

---

[1]) Tables des diviseurs pour tous les nombres des 1e, 2e et 3e millions. Paris 1814—17.

[2]) Faktortafeln für alle Zahlen der siebenten, achten und neunten Million; Hamburg 1862—65.

[3]) Factor table for the fourth, fifth and sixth million; London 1879—83.

[4]) Acta mathematica, Bd. 17, p. 301—314; 1893 (Afhandlingen er udgiven af *J. P. Gram*).

[5]) Factor table for the first ten millions. Washington 1909.

[6]) Efter en mundtlig meddelelse af *N. P. Bertelsen.*

[7]) Se Jahrbuch über die Fortschritte der Mathematik, Bd. 9 (1877), p. 115—116. Bd. 10 (1878), p. 124—125. Sammenlign *E. Lucas* sidstnævnte sted, p. 125.

[8]) Jahrbuch, Bd. 10 (1878), p. 123—124.

polynomiet $x^2 + x + 41$ giver lutter primtal for $0 \leqq x \leqq 39$
» $x^2 + x + 17$ » » » » $0 \leqq x \leqq 15$
» $2x^2 + 29$ » » » » $0 \leqq x \leqq 28$;

den første af disse angivelser skyldes *Euler*[1]), de to andre *Legendre*[2]); sammenlign forøvrig nedenstaaende opgave nr. 25 og *Wertheims* sidste skrift[3]).

Goldbach[4]) hævdede, at ethvert lige tal paa mindst en maade kan skrives som en sum af to primtal; men det er hidtil hverken lykkedes at bevise eller at modbevise dette postulat.

Af forfattere, som teoretisk har undersøgt *Goldbachs* postulat, vil vi her nævne *Stäckel*[5]), medens *G. Cantor*[6]) og *Haussner*[7]) har givet tabeller for de mindste lige tals fremstilling efter *Goldbachs* regel.

I disse tabeller vokser antallet af muligheder for et lige tals opløsning i en sum af to primtal med det lige tal.

Men heraf tør vi hverken drage slutninger for eller imod rigtigheden af *Goldbachs* postulat; ti i talteorien er intet tal, som vi kan behandle, et *stort* tal. *Legendre*[8]) bemærker i den henseende træffende, at man vilde tage meget fejl, hvis man f. eks. ved forsøg lod sig føre til det resultat, at ligningen

$$x^2 - 991y^2 = 1$$

ikke skulde kunne løses i hele tal for x og y; ti de mindste positive hele løsninger er

$$x = 379\,516\,400\,906\,811\,930\,638\,014\,896\,080$$
$$y = 12\,055\,735\,790\,331\,359\,447\,442\,538\,767.$$

---

[1]) Histoire de l'Académie de Berlin 1772, p. 36; (1774).
[2]) Théorie des nombres, Bd. I, p. 13. Zahlentheorie, Bd. I, p. 14.
[3]) Anfangsgründe der Zahlenlehre, p. 14; Braunschweig 1902.
[4]) *L. Euler*: Correspondance mathématique et physique, Bd. I, p. 135; St. Petersborg 1842.
[5]) Göttinger Nachrichten 1896, p. 292—299.
[6]) Association Française, congrès Caen 1894, p. 117—134; 1895.
[7]) Jahresbericht der deutschen Mathematiker-Vereinigung, Bd. 5, p. 62—66; 1887. Nova Acta der Leopoldinisch-Carolinischen Akademie, Bd. 72, p. 1—214; 1897.
[8]) Théorie des nombres, Bd. I, p. 58. Zahlentheorie, Bd. I, p. 59.

25. Bevis, at der ikke eksisterer noget helt polynomium

$$f(x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n,$$

som for alle positive hele værdier af x fremstiller lutter primtal.

§ 9. Eratostenes's sigte. Legendres regel.

Da man ikke kender noget simpelt udtryk for den lov, hvorefter primtallene forekommer i talrækken, kan man kun ved forsøg afgøre, om et forelagt tal er et primtal eller ikke.

Til praktisk opsøgelse af primtallene i talrækken haves allerede fra oldtiden en simpel metode, der efter sin opfinder sædvanlig kaldes *Eratostenes's* sigte (cribrum Eratosthenis).

Opskrives de hele tal større end 1 i naturlig rækkefølge, er det første af disse tal, nemlig 2, et primtal. Slettes hvert andet af tallene, idet man begynder med 2, er det første af de tiloversblevne tal, nemlig 3, et primtal. Slettes dernæst hvert tredje af tallene, idet man begynder med 3 og stadig medregner de alt ved 2 slettede tal, bliver det første af de tiloversblevne tal, nemlig 5, et primtal, o. s. v.

Langt senere har *Legendre*[1]) angivet følgende regel:

I. *Tallet p er et primtal, hvis det ikke er deleligt med noget primtal mindre end $\sqrt{p}$.*

Det er nemlig klart, at p maa være et primtal, hvis det ikke er deleligt med noget andet primtal. Lad os da antage, at vi ved forsøg har godtgjort, at intet primtal mindre end $\sqrt{p}$ gaar op i p; da kan p heller ikke være deleligt med noget primtal større end $\sqrt{p}$. Havdes nemlig $p = q \cdot r$, hvor $q > \sqrt{p}$, fik man $r < \sqrt{p}$; men det er umuligt; ti intet primtal, og altsaa heller intet sammensat tal mindre end $\sqrt{p}$ gaar op i p.

Vi bemærker, at *Wilsons* sætning giver os et teoretisk sikkert, men praktisk uanvendeligt middel til at afgøre, om et forelagt tal er et primtal eller ikke.

---

[1]) Théorie des nombres, Bd. I, p. 5—6. Zahlentheorie, Bd. I, p. 5—6.

26. Hvilke primtal faar man altid udskilt ved *Eratostenes's* sigte, naar man af talrækkens tal har slettet alle multipla af de $n-1$ første primtal $p_1, p_2, p_3, \ldots, p_{n-1}$?

27. Deles de n første primtal $p_1, p_2, \ldots, p_n$ i hvilkesomhelst to grupper $t_1, t_2, \ldots, t_r$ og $\tau_1, \tau_2, \ldots, \tau_s$, hvor $r+s=n$, og er $a_1, a_2, \ldots, a_r$, $\alpha_1, \alpha_2, \ldots, \alpha_s$ positive hele tal, da er alle positive hele tal af formen

$$\pm t_1^{a_1} t_2^{a_2} \cdots t_r^{a_r} \pm \tau_1^{\alpha_1} \tau_2^{\alpha_2} \cdots \tau_s^{\alpha_s}$$

og mindre end p_n^2 primtal [1]).

KAPITEL III.

Sammensatte tal.

§ 10. Antal og sum af et tals divisorer.

Et primtal p har ialt kun to divisorer, nemlig 1 og p; om sammensatte tal gælder sætningerne:

I. *Antallet* $\tau(n)$ *af divisorer i tallet*

$$n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}, \tag{1}$$

hvor $p_1, p_2, \ldots p_r$ *er forskellige primtal, bliver, idet* 1 *og* n *selv medregnes,*

$$\tau(n) = (a_1+1)(a_2+1)\cdots(a_r+1). \tag{2}$$

En hvilkensomhelst faktor i n kan ikke indeholde andre primfaktorer end saadanne, der forekommer i n selv; enhver divisor i n kan derfor skrives paa formen

$$p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}, \tag{3}$$

hvor

[1]) Denne opgave er meddelt mig af en tilhører ved forelæsningen.

(4) $$0 \leqq \alpha_1 \leqq a_1, \quad 0 \leqq \alpha_2 \leqq a_2, \quad \ldots, \quad 0 \leqq \alpha_r \leqq a_r,$$

og eksponenterne i (3) kan derfor ialt have henholdsvis

$$a_1 + 1, \; a_2 + 1, \; \ldots, \; a_r + 1$$

forskellige værdier, hvoraf (2) umiddelbart udledes.

Man ser, at tallet $\tau(n)$ altid er lige, undtagen naar n er et kvadrattal; af alikvote dele har tallet n ialt $\tau(n) - 1$.

II. *Summen* $\sigma(n)$ *af samtlige* $\tau(n)$ *divisorer i tallet* n, *bestemt ved produktet* (1), *bliver*

(5) $$\sigma(n) = \frac{p_1^{a_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{a_2+1} - 1}{p_2 - 1} \cdot \ldots \cdot \frac{p_r^{a_r+1} - 1}{p_r - 1}.$$

Er $n = p^a$ potensen af et primtal, bliver de $\tau(n)$ divisorer

$$1, \; p, \; p^2, \; \ldots, \; p^{a-1}, \; p^a,$$

og altsaa findes i dette tilfælde

$$\sigma(n) = 1 + p + p^2 + \cdots + p^a = \frac{p^{a+1} - 1}{p - 1},$$

og formlen (5) gælder saaledes for $r = 1$.

Lad os dernæst antage (5) gyldig for tallet med $r - 1$ primfaktorer

$$n_1 = p_2^{\alpha_2} p_3^{\alpha_3} \cdots p_r^{\alpha_r}, \quad n = n_1 p_1^{\alpha_1},$$

og lad os i (3) tillægge α_1 alle sine mulige værdier, medens $\alpha_2, \alpha_3, \ldots, \alpha_r$ hver for sig beholder en bestemt værdi; da bliver summen af de saaledes dannede $a_1 + 1$ divisorer i n bestemt ved

(6) $$p_2^{\alpha_2} p_3^{\alpha_3} \cdots p_r^{\alpha_r} \cdot \frac{p_1^{a_1+1} - 1}{p_1 - 1}.$$

Lader man endelig i denne sum eksponenterne $\alpha_2, \alpha_3, \ldots, \alpha_r$ efterhaanden antage alle deres mulige værdier, og adderes alle de saaledes af (6) erholdte udtryk, findes

$$\sigma(n) = \sigma(n_1) \frac{p_1^{a_1+1} - 1}{p_1 - 1},$$

og altsaa er formlen (5) almengyldig.

Af identiteten

$$1 + p + p^2 + \cdots + p^a = p^a\left(1 + \frac{1}{p} + \frac{1}{p^2} + \cdots + \frac{1}{p^a}\right)$$

slutter man, at

$$\frac{p^{a+1} - 1}{p - 1} \geqq p^a\left(1 + \frac{1}{p}\right), \tag{7}$$

hvor ligheden kun er mulig for $a = 1$. Af denne bemærkning findes for faktorsummen $\sigma(n)$:

$$\sigma(n) \geqq n\left(1 + \frac{1}{p_1}\right)\left(1 + \frac{1}{p_2}\right)\cdots\left(1 + \frac{1}{p_r}\right), \tag{8}$$

hvor ligheden ifølge (7) kun er mulig, naar

$$a_1 = a_2 = a_3 = \cdots = a_r = 1,$$

altsaa naar tallet n er et produkt af lutter forskellige primtal.

Udføres multiplikationerne paa højre side i (8), findes endvidere

$$\sigma(n) \geqq n\left(1 + \frac{1}{p_1} + \frac{1}{p_2} + \cdots + \frac{1}{p_r}\right), \tag{9}$$

hvor ligheden kun er mulig, naar $r = 1$, altsaa naar $n = p$ er et primtal.

---

28. Betegner $d_1, d_2, \ldots, d_m$ samtlige divisorer i tallet a, er altsaa $m = \tau(a)$, haves
$$a^m = (d_1 d_2 \cdots d_m)^2.$$
29. Bevis, at tallene p^3, hvor p er et primtal, og pq, hvor p og q er forskellige primtal, er de eneste hele tal, der er lig med produktet af deres alikvote dele[1]).
30. Bevis, at ethvert helt tal, som ikke er af formen $4n + 2$, kan skrives som en differens af to kvadrattal, og angiv, paa hvor mange maader en saadan fremstilling er mulig.
31. Hvorledes løses opg. 30, naar intet af de to kvadrattal maa være 0?

---

[1]) *E. Lionnet* i Nouvelles Annales (2) Bd. 18, p. 306—308; 1879.

§ 11. Den Eulerske funktion $\varphi(n)$.

Om antallet af de positive hele tal, der er mindre end eller lig med tallet n og indbyrdes primiske med n, haves følgende sætning af *Euler*[1]:

I. *Antallet* $\varphi(n)$ *af de tal, der er mindre end eller lig med* n *og indbyrdes primiske med* n, *som opløst i sine primfaktorer er*

$$(1) \qquad n = p_1^{a_1} p_2^{a_2} \cdot \cdots \cdot p_r^{a_r},$$

bestemmes ved udtrykket

$$(2) \quad \varphi(n) = p_1^{a_1-1}(p_1 - 1) p_2^{a_2-1}(p_2 - 1) \cdot \cdots \cdot p_r^{a_r-1}(p_r - 1)$$

eller

$$(3) \qquad \varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdot \cdots \cdot \left(1 - \frac{1}{p_r}\right).$$

Da q og $np + q$, hvor p er et vilkaarligt helt tal, samtidig er indbyrdes primiske med n eller ikke, maa der mellem to paa hinanden følgende multipla af n findes netop $\varphi(n)$ tal, der er primiske med n. Betegner p et positivt helt tal, er antallet af positive hele tal, der er mindre end eller lig med np og primiske med n, netop $p \cdot \varphi(n)$.

Ved hjælp af disse bemærkninger bevises I uden vanskelighed ved induktion.

Er først $n = p^a$ en primtalpotens, findes der mellem o og n følgende multipla af p:

$$p,\ 2p,\ 3p,\ \ldots,\ p \cdot p^{a-1};$$

da antallet af disse multipla er p^{a-1}, haves derfor i dette tilfælde

$$\varphi(n) = p^a - p^{a-1} = p^{a-1}(p - 1) = n\left(1 - \frac{1}{p}\right).$$

Lad os dernæst antage, at I gjaldt for tallet

$$(4) \qquad n_1 = p_2^{a_2} p_3^{a_3} \cdot \cdots \cdot p_r^{a_r}, \quad n = n_1 p_1^{a_1},$$

[1]) Novi Commentarii Academiæ Petropolitanæ, Bd. 8, p. 74—104; 1760—61 (1763). Acta Academiæ Petropolitanæ, 1780 II, p. 18—30; 1784. Commentationes arithmeticæ collectæ, Bd. I, p. 274—286; St. Petersborg 1849.

med $r - 1$ primfaktorer; det er da for det første klart, at alle multipla af primtallet p_1, som ikke er større end n, bliver

$$p_1,\ 2p_1,\ 3p_1,\ \ldots\ldots,\ \frac{n}{p_1}\cdot p_1;$$

for det andet bliver antallet af disse multipla, som ikke tillige er delelige med noget af primtallene $p_2,\ p_3,\ \ldots\ldots,\ p_r$, netop $p_1^{a_1-1}\varphi(n_1)$; det samlede antal af positive hele tal, som ikke overskrider n og er indbyrdes primiske med n, bliver derfor

$$\varphi(n) = p_1^{a_1}\varphi(n_1) - p_1^{a_1-1}\varphi(n_1) = p_1^{a_1-1}(p_1 - 1)\varphi(n_1),$$

hvilket netop er udtrykket (2).

Af det saaledes beviste udtryk for $\varphi(n)$ faas umiddelbart følgende sætning:

II. *Antages a og b indbyrdes primiske, er*

$$\varphi(a)\,\varphi(b) = \varphi(ab). \tag{5}$$

Om funktionen $\varphi(n)$ haves endvidere følgende sætning af *Gauss*[1]):

III. *Betegner $d_1, d_2, d_3, \ldots\ldots, d_m$ samtlige divisorer i tallet n, altsaa $m = \tau(n)$, og sættes $\varphi(1) = 1$, haves*

$$\varphi(d_1) + \varphi(d_2) + \cdots\cdots + \varphi(d_m) = n. \tag{6}$$

Betragtes først primtalpotensen $n = p^a$, bliver alle divisorerne

$$1,\ p,\ p^2,\ \ldots\ldots,\ p^a,$$

og for summen af de tilsvarende φ-funktioner findes

$$1 + (p-1) + p(p-1) + \cdots\cdots + p^{a-1}(p-1) = \\ = 1 + p^a - 1 = p^a = n.$$

Lad dernæst n_1 være det i (4) definerede tal med $r - 1$ primfaktorer, og lad samtlige divisorer i n_1 være $d'_1, d'_2, \ldots\ldots, d'_q$; da antager vi, at

$$\varphi(d'_1) + \varphi(d'_2) + \cdots\cdots + \varphi(d'_q) = n_1. \tag{7}$$

[1]) Disquisitiones arithmeticæ, art. 39 Werke, Bd. I, p. 31—32. Untersuchungen über höhere Arithmetik, p. 23—24; Berlin 1889.

Samtlige divisorer i tallet n fremstilles ved produkterne

(8) $$p_1^{\alpha_1} d'_s, \quad 1 \leqq s \leqq q, \quad 0 \leqq \alpha_1 \leqq a_1;$$

holdes i produktet (8) faktoren d'_s fast, medens α_1 varierer, bliver summen af de saaledes dannede faktorers φ-funktioner ifølge (5)

(9) $$p_1^{\alpha_1} \varphi(d'_s);$$

lader man dernæst i (9) s gennemløbe alle sine mulige værdier, faas ifølge (7)

$$\varphi(d_1) + \varphi(d_2) + \cdots \varphi(d_m) = p_1^{\alpha_1} n_1 = n.$$

---

32. Man skal for ethvert lige n bevise, at $\varphi(n) \leqq \frac{1}{2}n$, og angive de n, for hvilke ligheden finder sted.
33. Indeholder det ulige tal n kun højst to forskellige primfaktorer, haves stedse $\varphi(n) > \frac{1}{2}n$.
34. Hvis primtalmængden antoges endelig, og samtlige primtal var $p_1, p_2, \ldots, p_n$, kommer man til en absurditet ved at undersøge funktionen

$$\varphi(p_1 p_2 \cdots p_n)\ ^{1}).$$

35. Find summen af tallene mindre end n og primiske med n.

§ 12. Opløsning i primfaktorer af $n!$

Idet n er positiv hel, vil vi søge at opløse tallet

$$1 \cdot 2 \cdot 3 \cdots n = n!$$

i primfaktorer. I dette øjemed betegner vi ved p et vilkaarligt primtal, saaledes at $p \leqq n$, og skriver dernæst n i p-talsystemet; altsaa

(1) $$n = a_r p^r + a_{r-1} p^{r-1} + \cdots + a_1 p + a_0.$$

---

[1]) *Kummer* i Berliner Monatsberichte 1878, p. 777—778.

Alle multipla af p^m, hvor $m \leqq r$, mindre end n er altsaa

$$p^m,\ 2p^m,\ 3p^m,\ \ldots,\ (a_r p^{r-m} + a_{r-1}p^{r-m-1} + \cdots + a_m)p^m,$$

og den bestemte potens p^m forekommer derfor ialt

$$A_m = a_r p^{r-m} + a_{r-1}p^{r-m-1} + \cdots + a_m \tag{2}$$

gange som faktorer i $n!$.

Sættes dernæst i (2) $m = 1, 2, 3, \ldots, r$, og adderes alle de saaledes erholdte ligninger, angiver denne sum eksponenten til den højeste potens af primtallet p, som gaar op i $n!$ Ti de tal, der er mindre end eller lig med n og delelige med p^q, medregnes netop q gange i ovennævnte sum, nemlig hidrørende fra $A_1, A_2, A_3, \ldots, A_q$. Eksponenten til den højeste potens af p, som gaar op i $n!$, bliver derfor

$$\varepsilon = A_1 + A_2 + \cdots + A_r,$$

hvoraf ved indførelse af udtrykkene (2)

$$\varepsilon = a_r\frac{p^r - 1}{p-1} + a_{r-1}\frac{p^{r-1}-1}{p-1} + \cdots + a_1\frac{p-1}{p-1} + a_0\frac{1-1}{p-1},$$

og altsaa findes

$$\varepsilon = \frac{a_r p^r + a_{r-1}p^{r-1} + \cdots + a_1 p + a_0 - (a_r + a_{r-1} + \cdots + a_1 + a_0)}{p-1}$$

eller [1])

$$\varepsilon = \frac{n - t_p(n)}{p-1}, \tag{3}$$

og altsaa har vi bevist sætningen:

I. *Betegner $p_1, p_2, \ldots, p_m$ samtlige primtal mindre end eller lig med n, og er ε_q det af* (3) *dannede udtryk, idet vi istedetfor p indfører p_q, haves*

$$n! = p_1^{\varepsilon_1} p_2^{\varepsilon_2} \cdots p_m^{\varepsilon_m}. \tag{4}$$

---

[1]) Sammenlign *Legendre*: Théorie des nombres, Bd. I, p. 12. Zahlentheorie, Bd. I, p. 12.

Løsning af 38. Er a et vilkaarligt primtal, skal man altsaa bevise, at

$$t_a(n) + t_a(p) + t_a(n+p) - t_a(2n) - t_a(2p) \geqq 0.$$

Antages $a = 2$, haves

$$t_2(2n) = t_2(n), \quad t_2(2p) = t_2(p),$$

saaledes at overstaaende uttryk i dette tilfælde bliver $t_2(n+p)$.

Er a et uligt primtal, og antages samtlige cifre i n og p mindre end $\frac{a}{2}$, haves

$$t_a(2n) = 2t_a(n), \quad t_a(2p) = 2t_a(p), \quad t_a(n+p) = t_a(n) + t_a(p),$$

saaledes at overstaaende uttryk i dette tilfælde er 0.

Er blot ciffer i n eller p, der er større end $\frac{a}{2}$, bliver $t_a(2n)$ eller $t_a(2p)$ formindsket med $a-1$; dette kan muligvis ogsaa finde sted for summen af de tilsvarende cifre i $t_a(n+p)$, saaledes at uttrykket overfor enten bliver uforandret eller forøget $a-1$.

Da ifølge § 6, (7) bestandig

$$t_p(a) + t_p(b) \geqq t_p(a+b), \tag{5}$$

faas den om polynomialkoefficienterne velkendte sætning:

II. *Betegner $a_1, a_2, a_3, \ldots, a_n$, vilkaarlige positive hele tal, er kvotienten*

$$\frac{(a_1 + a_2 + a_3 + \cdots + a_n)!}{a_1!\, a_2!\, a_3! \cdots a_n!} \tag{6}$$

altid et helt tal.

Ethvert primtal, der forekommer som faktor i nævneren i (6), maa nemlig ifølge (3) og (5) forekomme mindst lige saa hyppig som faktor i tælleren.

Specielt faas af II ved anvendelse af § 3, VI:

III. *Er p et primtal, og $1 \leqq r \leqq p-1$, haves bestandig*

$$\binom{p}{r} = \frac{p!}{r!\,(p-r)!} \equiv 0 \pmod{p}. \tag{7}$$

Ti primtallet p, der findes som faktor i tælleren, er primisk med nævneren, fordi $p > r$ og $p > p - r$.

---

36. Sættes $n = 2^p$, skal man bevise, at $\binom{2n}{n}$ er et tal af formen $4k+2$.

37. Idet n, p og q er positive hele, og $1 \leqq q \leqq p-1$, skal man bevise, at produktet

$$n(n+1)\cdots(n+q-1)\cdot$$
$$\cdot(1+(p-1)n)(2+(p-1)n)\cdots(p-q+(p-1)n)$$

altid er deleligt med $p!$

38. Betegner n og p vilkaarlige positive hele tal, er kvotienten

$$\frac{(2n)!\,(2p)!}{n!\,p!\,(n+p)!}$$

altid et helt tal [1]).

---

[1]) *Catalan* i Nouvelles Annales (2) Bd. 13, p. 207; 1874. *P. Bachmann* i Zeitschrift für Mathematik und Physik, Bd. 20, p. 161; 1874. *Bourguet* i Nouvelles Annales (2) Bd. 14, p. 89—90; 1875.

39. Bevis, at, hvis m og n er positive hele, indbyrdes primiske tal, er

$$\frac{(m+n-1)!}{m!\,n!}$$

altid et helt tal [1]).

40. Find den højeste potens af primtallet a, som gaar op i produktet

$$n(n+1)(n+2)\cdots(na-1),$$

hvor n er et positivt helt tal [2]).

KAPITEL IV.

Fuldkomne og venskabelige tal.

§ 13. Sætninger om fuldkomne tal.

Et tal, der er lig med sin halve divisorsum, kaldes fuldkomment; er n et saadant tal, haves altsaa

$$2n = \sigma(n); \tag{1}$$

da 1 regnes med til de alikvote dele af et tal, kan man derfor sige, at et fuldkomment tal er lig med summen af sine alikvote dele.

Om fuldkomne tal har allerede *Euklid* givet sætningen:

I. *Saafremt* $2^n - 1$ *er et primtal, er*

$$e_n = 2^{n-1}(2^n - 1) \tag{2}$$

et fuldkomment tal.

---

[1]) *Catalan* i Nouvelles Annales (2) Bd. 13, p. 523; 1874.

[2]) Videre undersøgelser findes i Nouvelles Annales (2) Bd. 11, p. 314—319; 1872.

Da $2^n - 1$ er et primtal, kan samtlige divisorer i e_n deles i to klasser, nemlig

$$1,\ 2,\ 2^2,\ 2^3,\ \cdots,\ 2^{n-1}$$
$$2^n - 1,\ 2(2^n - 1),\ \cdots,\ 2^{n-1}(2^n - 1),$$

og summen af disse to klasser bliver henholdsvis

$$2^n - 1,\ (2^n - 1)^2,$$

og altsaa haves

$$2e_n = \sigma(e_n).$$

Euler[1]) har bevist den til I svarende omvendte sætning, nemlig:

II. *De af Euklid angivne er de eneste eksisterende lige fuldkomne tal.*

Er nemlig det lige tal

$$A = 2^\alpha p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r} = 2^\alpha K, \tag{3}$$

hvor $p_1, p_2, \ldots, p_r$ er indbyrdes forskellige ulige primtal, et fuldkomment tal, haves ifølge (1):

$$2A = 2^{\alpha+1}K = \sigma(A) = (2^{\alpha+1} - 1)\,\sigma(K),$$

hvoraf ved anvendelse § 10, (9) og efter en simpel omskrivning

$$\left\{\begin{array}{l} (2^{\alpha+1} - 1)K + K = \\ = (2^{\alpha+1} - 1)\,\sigma(K) \geqq (2^{\alpha+1} - 1)K\left(1 + \frac{1}{p_1}\right), \end{array}\right. \tag{4}$$

hvor p_1 er det mindste ulige primtal, der gaar op i A og derfor ogsaa i K. Af (4) findes imidlertid

$$K + \frac{K}{2^{\alpha+1} - 1} = \sigma(K) \geqq K + \frac{K}{p_1}.$$

Da $\sigma(K)$ er et helt tal, slutter man heraf, at $2^{\alpha+1} - 1$ maa gaa op i K, og altsaa haves $2^{\alpha+1} - 1 \geqq p_1$; ti p_1 er det mindste ulige primtal, der gaar op i K, altsaa er p_1 tillige

[1]) Commentationes arithmeticæ collectæ, Bd. II, pp. 514, 630; St. Petersborg 1849.

den mindste divisor i K større end 1. Da man ikke desto mindre skal have

$$\frac{K}{2^{a+1}-1} \geqq \frac{K}{p_1},$$

maa K være selve primtallet p_1, og endvidere haves

$$p_1 = 2^{a+1} - 1.$$

Tallet A maa derfor være af formen (2).

J. Carvallo [1]) har forsøgt at bevise, at der ikke eksisterer *ulige* fuldkomne tal; men hans bevis er ikke nøjagtigt.

Derimod haves om disse hypotetiske tal følgende sætning af *Euler* [2]):

III. *Et ulige fuldkomment tal A maa altid, hvis det eksisterer, være af formen*

$$A = (4p+1)^{4a+1} \cdot N^2, \tag{4}$$

hvor $4p+1$ *er et primtal, der ikke gaar op i det ulige tal* N.

Tænkes det eventuelle ulige fuldkomne tal A opløst i primfaktorer at være

$$A = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r},$$

haves altsaa

$$2A = \frac{p_1^{a_1+1}-1}{p_1-1} \cdot \frac{p_2^{a_2+1}-1}{p_2-1} \cdots \frac{p_r^{a_r+1}-1}{p_r-1}. \tag{5}$$

Er nu p et ulige tal, og sættes

$$P = \frac{p^{a+1}-1}{p-1} = (1 + p + p^2 + \cdots + p^a), \tag{6}$$

er P da og kun da ulige, naar a er et lige tal; ti i dette tilfælde indeholder summen paa højre side i (6) et ulige antal addender, der alle er ulige tal, og altsaa er P selv et ulige tal. Antages derimod a ulige, og sættes $a = 2r - 1$, faas

---

[1]) Comptes rendus, Bd. 81, p. 73—75; 1875. Théorie des nombres parfaits. Barcelona 1883.

[2]) Commentationes arithmeticæ collectæ, Bd. II, p. 515; St. Petersborg 1849.

den mindste divisor i K større end 1. Da man ikke desto mindre skal have

$$\frac{K}{2^{a+1}-1} \geqq \frac{K}{p_1},$$

maa K være selve primtallet p_1, og endvidere haves

$$p_1 = 2^{a+1} - 1.$$

Tallet A maa derfor være af formen (2).

F. Carvallo [1]) har forsøgt at bevise, at der ikke eksisterer *ulige* fuldkomne tal; men hans bevis er ikke nøjagtigt.

Derimod haves om disse hypotetiske tal følgende sætning af *Euler* [2]):

III. *Et ulige fuldkomment tal A maa altid, hvis det eksisterer, være af formen*

$$A = (4p + 1)^{4a+1} \cdot N^2, \tag{4}$$

hvor $4p + 1$ *er et primtal, der ikke gaar op i det ulige tal* N.

Tænkes det eventuelle ulige fuldkomne tal A opløst i primfaktorer at være

$$A = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r},$$

haves altsaa

$$2A = \frac{p_1^{a_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{a_2+1} - 1}{p_2 - 1} \cdots \frac{p_r^{a_r+1} - 1}{p_r - 1}. \tag{5}$$

Er nu p et ulige tal, og sættes

$$P = \frac{p^{a+1} - 1}{p - 1} = (1 + p + p^2 + \cdots + p^a), \tag{6}$$

er P da og kun da ulige, naar a er et lige tal; ti i dette tilfælde indeholder summen paa højre side i (6) et ulige antal addender, der alle er ulige tal, og altsaa er P selv et ulige tal. Antages derimod a ulige, og sættes $a = 2r - 1$, faas

---

[1]) Comptes rendus, Bd. 81, p. 73—75; 1875. Théorie des nombres parfaits. Barcelona 1883.

[2]) Commentationes arithmeticæ collectæ, Bd. II, p. 515; St. Petersborg 1849.

$$(7) \quad P = \frac{p^{2r} - 1}{p - 1} = (p + 1)(p^{2r-2} + p^{2r-4} + \cdots + p^2 + 1),$$

og altsaa er P et lige tal.

Da nu i (5) $2A$ skal være et tal af formen $4k + 2$, kan kun en af eksponenterne $a_1, a_2, \cdots, a_r$, være et ulige tal.

Skal dernæst i (6) P være af formen $4k + 2$, maa baade p og a være af formen $4m + 1$; er nemlig $p = 4m - 1$, $p + 1 = 4m$, bliver ifølge (7) P delelig med 4; er endvidere $a = 4m - 1$, faas

$$P = \frac{p^{4m} - 1}{p - 1} = (p + 1)(p^2 + 1)(p^{4m-4} + p^{4m-8} + \cdots + p^4 + 1),$$

og altsaa er i dette tilfælde P ligeledes delelig med 4.

Der kan altsaa i hvert fald ikke eksistere andre ulige fuldkomne tal end de i (4) angivne.

Da tallet i (4) altid maa være af formen $4n + 1$, faas endvidere sætningen:

IV. *Der eksisterer ingen fuldkomne tal af formen* $4n + 3$.

Da man hverken har kunnet angive noget ulige fuldkomment tal eller bevise, at disse tal ikke eksisterer, kender man i øjeblikket kun følgende 9 fuldkomne tal:

$$(8) \qquad e_2,\ e_3,\ e_5,\ e_7,\ e_{13},\ e_{17},\ e_{19},\ e_{31},\ e_{61},$$

eller udregnede:

$e_2 = 6$, $e_3 = 28$, $e_5 = 496$, $e_7 = 8128$, $e_{13} = 33\,550\,336$
$e_{17} = 8\,589\,869\,056$, $e_{19} = 137\,438\,691\,328$
$e_{31} = 2\,305\,843\,008\,139\,952\,128$
$e_{61} = 2\,658\,455\,991\,569\,831\,744\,654\,692\,615\,953\,842\,176$.

De første 8 kendtes allerede af *Euler*, medens *N. P. Bertelsen* har meddelt mig værdien af e_{61}. Som vi skal se i § 33, eksisterer der ikke andre lige fuldkomne tal mindre end e_{89} end de lige nævnte.

---

41. Bevis, at ethvert lige fuldkomment tal modulo 10 kun kan give den principale rest 8 eller 6.
42. Bevis, at ethvert lige fuldkomment tal, større end 6, modulo 9 giver den principale rest 1.

§ 14. Legendres undersøgelser over venskabelige tal.

To tal a og b kaldes venskabelige, naar ethvert af dem er lig med summen af det andets alikvote dele; altsaa naar man for divisorsummerne har

$$\sigma(a) = \sigma(b) = a + b. \tag{1}$$

Jamblikos fortæller, at allerede *Pytagoras* skal have kendt de to venskabelige tal

$$a = 220, \quad b = 284.$$

Den første almindeligere regel til dannelsen af venskabelige tal skyldes *Thâbit ibn Kurra;* denne regel er senere genfunden af *Descartes* og *Frenicle*, medens *Legendre* har generaliseret den.

Legendre[1]) søger at bestemme to venskabelige tal af formen

$$a = 2^n pq, \quad b = 2^n r, \tag{2}$$

hvor p, q og r er indbyrdes forskellige, ulige primtal; vi antager $p > q$. Af (2) findes

$$\sigma(a) = (2^{n+1} - 1)(p + 1)(q + 1), \ \sigma(b) = (2^{n+1} - 1)(r + 1),$$

og altsaa erholdes ifølge (1)

$$r = pq + p + q, \ (2^{n+1} - 1)(pq + p + q + 1) = 2^n(2pq + p + q).$$

Skrives den sidste af disse ligninger paa formen

$$(p - 2^n + 1)(q - 2^n + 1) = 2^{2n},$$

faas, idet α er positiv hel og mindre end n:

$$p - 2^n + 1 = 2^{n+\alpha}, \quad q - 2^n + 1 = 2^{n-\alpha},$$

og altsaa findes følgende mulige værdier for p, q og r

$$\begin{cases} p = (2^\alpha + 1)\,2^n - 1, \quad q = (2^\alpha + 1)\,2^{n-\alpha} - 1, \\ r = (2^\alpha + 1)^2\,2^{2n-\alpha} - 1; \end{cases} \tag{3}$$

[1]) Théorie des nombres, Bd. II, p. 148—150. Zahlentheorie, Bd. II, 143—146.

i disse udtryk kommer det derfor an paa at vælge n og α saaledes, at alle tre tal p, q og r bliver primtal.

Man ser straks, at α ikke kan være lige; ti saa blev r et tal af formen $s^2 - 1$ og følgelig intet primtal, fordi $s > 2$. Endvidere kan α ikke være 3; ti $2^3 + 1 = 9$, og et af tallene p og q blev da samtidig af formen $s^2 - 1$.

Sættes $\alpha = 1$, faas *Thâbit ibn Kurras* regel

$$(4) \quad p = 3 \cdot 2^n - 1, \quad q = 3 \cdot 2^{n-1} - 1, \quad r = 9 \cdot 2^{2n-1} - 1;$$

som *Le Lasseur*[1]) har vist, gives der blandt tallene (4) for $n < 35$ kun de tre løsninger

$$n = 2, \quad n = 4, \quad n = 7,$$

hvortil svarer venskabelige tal, nemlig

$$\begin{aligned} a &= 284, & b &= 220 \\ a &= 18\,416, & b &= 17\,296 \\ a &= 9\,437\,056, & b &= 9\,363\,584; \end{aligned}$$

det første af disse par kendtes allerede i oldtiden, medens de to andre er fundne af *Frans van Schooten*[2]).

Antagelsen $\alpha = 5$ giver ifølge (3)

$$(5) \quad p = 33 \cdot 2^n - 1, \quad q = 33 \cdot 2^{n-5} - 1, \quad r = 33^2 \cdot 2^{2n-5} - 1;$$

men man synes ikke at kende nogen værdi af n, for hvilken disse tal p, q og r alle er primtal.

Sættes $\alpha = 7$, faas paa lignende maade

$$(6) \quad p = 129 \cdot 2^n - 1, \quad q = 129 \cdot 2^{n-7} - 1, \quad r = 129^2 \cdot 2^{2n-7} - 1;$$

for $n = 8$ faas herved efter *Seelhoff*[3]) de to venskabelige tal

$$a = 2\,181\,168\,896, \quad b = 2\,172\,649\,216.$$

---

[1]) *Lucas:* Théorie des nombres, Bd. I, p. 381; Paris 1891.
[2]) Exercitationes mathematicæ, lib. V, p. 423; Leiden 1657.
[3]) Archiv der Mathematik und Physik, Bd. 70, p. 78; 1883.

§ 15. Eulers og Seelhoffs undersøgelser over venskabelige tal.

Legendres metode til bestemmelse af venskabelige tal kan generaliseres, idet man søger tal af formen

$$a = fpq, \quad b = fr, \tag{1}$$

hvor p, q og r skal være forskellige primtal, saaledes at f er største fælles faktor for a og b.

Sættes for kortheds skyld

$$\sigma(f) = F, \tag{2}$$

og skal tallene i (1) være venskabelige, finder man som før

$$r = pq + p + q, \quad (p+1)(q+1)F = (pq+r)f. \tag{3}$$

For at løse de ubestemte ligninger (3) opgiver *Euler*[1]) tallene p og q og søger at bestemme f og r, medens *Seelhoff*[2]) opgiver f og søger at bestemme primtallene p, q og r.

Elimineres r af ligningerne (3), kan den derved fundne ligning bringes paa formen

$$(p+1)(q+1) = \frac{f}{2f-F}(p+1) + \frac{f}{2f-F}(q+1)$$

eller efter en simpel omskrivning

$$\left(p+1-\frac{f}{2f-F}\right)\left(q+1-\frac{f}{2f-F}\right) = \frac{f^2}{(2f-F)^2}. \tag{4}$$

Vælges dernæst tallene g og h, saaledes at

$$gh = f^2, \tag{5}$$

er (4) aabenbart tilfredsstillet, naar

$$p+1 = \frac{f+g}{2f-F}, \quad q+1 = \frac{f+h}{2f-F}. \tag{6}$$

---

[1]) Opuscula varii argumenti, Bd. II, p. 23—107; Berlin 1750. Commentationes arithmeticæ collectæ, Bd. II, p. 627—638; St. Petersborg 1849. Opera postuma, Bd. I, p. 85—100; St. Petersborg 1862.

[2]) Archiv der Mathematik und Physik, Bd. 70, p. 75—89; 1883.

Opgives f, kommer det derfor an paa at bestemme g og h, saaledes at de i (6) angivne tal p og q begge bliver primtal, der tilfredsstiller den betingelse, at $r = pq + p + q$ ligeledes er et primtal.

Sættes f. eks.

$$f = 3^2 \cdot 7^2 \cdot 13 \cdot 19 \cdot 23,$$

finder man

$$F = 13 \cdot 57 \cdot 14 \cdot 20 \cdot 24, \quad \frac{f}{2f - F} = \frac{161}{2};$$

vælges dernæst

$$g = 7, \quad h = 7 \cdot 23^2 = 3703,$$

finder man

$$p + 1 = \frac{161 + 7}{2} = 84, \quad q + 1 = \frac{161 + 2703}{2} = 1932, \quad r = 162287,$$

og de tilsvarende venskabelige tal bliver

$$a = 3^2 \cdot 7^2 \cdot 13 \cdot 19 \cdot 23 \cdot 83 \cdot 1931$$
$$b = 3^2 \cdot 7^2 \cdot 13 \cdot 19 \cdot 23 \cdot 162287.$$

Sættes $f = 2^n$, genfindes den i foregaaende paragraf udviklede metode.

Euler fandt 61, *Seelhoff* desuden nogle andre par af venskabelige tal.

KAPITEL V.

Talteoretiske funktioner.

§ 16. Eksempler. Potenssummer og fakultetkoefficienter.

En hvilkensomhelst funktion $f(x)$, der er defineret for positive hele værdier af sit argument x, kaldes en talteoretisk funktion.

Ved vor behandling af sammensatte tals divisorer har vi allerede betragtet enkelte talteoretiske funktioner, nemlig:

Eks. 1. Antallet af divisorer i tallet n, der betegnedes $\tau(n)$; den nødvendige og tilstrækkelige betingelse for, at p er et primtal, bliver derfor $\tau(n) = 2$.

Eks. 2. Summen af samtlige divisorer i n, der betegnedes $\sigma(n)$; man har derfor stedse $\sigma(n) \geqq n + 1$, hvor ligheden kun er mulig, naar n er et primtal.

Eks. 3. Den *Eulerske* funktion $\varphi(n)$, der betegner antallet af tal mindre end eller lig med n og indbyrdes primiske med n. For $n > 1$ haves derfor stedse $\varphi(n) \leqq n - 1$, og ligheden er kun mulig, naar n er et primtal.

Af andre talteoretiske funktioner, der ikke er behandlede i det foregaaende, vil vi her endnu nævne følgende:

Eks. 4. Den saakaldte *Möbius'ske*[1]) faktor $\mu(n)$, der for $n > 1$ defineres saaledes, at $\mu(n) = 0$, naar n er deleligt med et kvadrat større end 1, og at $\mu(n) = (-1)^m$, naar n er produktet af m forskellige primtal.

Eks. 5. Funktionen $\delta(n)$, der er lig antallet af maader, paa hvilke tallet n kan skrives som en sum af positive hele tal.

Betegner $\delta'(n)$ og $\delta''(n)$ antallet af maader, paa hvilke n kan skrives som en sum af positive hele tal, der alle er henholdsvis lige eller ulige, haves derfor stedse $\delta(n) \geqq \delta'(n) + \delta''(n)$.

Eks. 6. $n! = 1 \cdot 2 \cdot 3 \cdot \cdots \cdot n$.

De lige nævnte talteoretiske funktioner har alle kun et argument; som eksempler paa talteoretiske funktioner af to variable vil vi nævne følgende:

Eks. 7. *Potenssummer af talrækkens tal.* Idet n og p er positive hele tal, sætter vi

$$(1) \qquad 1^p + 2^p + 3^p + \cdots + n^p = S_p(n);$$

denne sum har derfor de to argumenter n og p.

Eks. 8. *Fakultetkoefficienterne.* Betegner n et positivt helt tal, kaldes produktet

---

[1]) Funktionen $\mu(n)$ omtales af *Möbius* i Crelles Journal, Bd. 9, p. 105—123; 1832. Tallet $\mu(n)$ er dog endnu tidligere betragtet af *Gauss* i Disquisitiones arithmeticæ, art. 81. Untersuchungen über höhere Arithmetik, p. 56; Berlin 1889. Werke, Bd. I, p. 62—64.

(2) $$\omega_n(x) = x(x+1)(x+2)\cdots(x+n-1)$$

et fakultet af n^{te} orden; for $x = 1$ findes umiddelbart

(3) $$\omega_n(1) = n!.$$

Udføres multiplikationerne paa højre side i (2), og sættes

(4) $$\omega_n(x) = C_n^0 x^n + C_n^1 x^{n-1} + \cdots + C_n^p x^{n-p} + \cdots + C_n^{n-1} x,$$

kaldes tallene C_n^p fakultetkoefficienterne af n^{te} orden, medens p er rangen af C_n^p. Rangen af en fakultetkoefficient er derfor altid mindre end dens orden. Man finder specielt

(5) $$C_n^0 = 1, \quad C_n^{n-1} = (n-1)!,$$

og almindelig haves sætningen:

I. *Fakultetkoefficienten C_n^p er summen af alle de produkter, der kan dannes af p forskellige faktorer udtagne af tallene* 1, 2, 3, $\cdots$, $n-1$. *Her maa man altsaa forudsætte*

$$1 \leqq p \leqq n-1.$$

Specielt findes

(6) $$C_n^1 = 1 + 2 + 3 + \cdots + (n-1) = \frac{n(n-1)}{2}.$$

Fakultetets definition giver umiddelbart identiteterne

(7) $$\omega_{n+1}(x) = (x+n)\,\omega_n(x) = x\,\omega_n(x+1).$$

Af det første af udtrykkene paa højre side i (7) finder man ved anvendelse af (4), idet man søger koefficienten til x^{n-p+1}

(8) $$C_{n+1}^p = C_n^p + nC_n^{p-1}, \quad 1 \leqq p \leqq n-1;$$

for de undtagne værdier $p = 0$ og $p = n$ finder man derimod henholdsvis

(9) $$C_{n+1}^0 = C_n^0 = 1, \quad C_{n+1}^n = nC_n^{n-1} = n!.$$

Søges i det andet af de i (7) givne udtryk,

$$\omega_{n+1}(x) = x\cdot\left(C_n^0(x+1)^n + C_n^1(x+1)^{n-1} + \cdots + C_n^{n-1}(x+1)\right),$$

ligeledes koefficienten til potensen x^{n-p+1}, findes denne paa højre side, idet man i potenserne

$$(x+1)^n, \quad (x+1)^{n-1}, \quad \cdots, \quad (x+1)^{n-p}$$

søger koefficienterne til x^{n-p}; da de tilsvarende binomialkoefficienter bliver

$$\binom{n}{p}, \quad \binom{n-1}{p-1}, \quad \cdots, \quad \binom{n-p}{0},$$

finder man paa denne maade formlerne

$$C_{n+1}^p = \binom{n}{p} C_n^0 + \binom{n-1}{p-1} C_n^1 + \cdots + \binom{n-p}{0} C_n^p,$$
$$0 \leqq p \leqq n-1.$$

Indføres her udtrykket (8), og bemærkes det, at C_n^p derefter falder bort, finder man for $1 \leqq p \leqq n-1$

$$n C_n^{p-1} = \binom{n}{p} C_n^0 + \binom{n-1}{p-1} C_n^1 + \cdots + \binom{n-p+1}{1} C_n^{p-1};$$

denne formel reduceres for $p = 1$ til en trivialitet. Antages $2 \leqq p \leqq n-1$, findes derimod

$$(10) \quad (p-1)\, C_n^{p-1} = \binom{n}{p} C_n^0 + \binom{n-1}{p-1} C_n^1 + \cdots + \binom{n-p+2}{2} C_n^{p-2}.$$

Af (2) og (4) faas den til (10) for $p = n$ svarende formel

$$(11) \quad (n-1)\, C_n^{n-1} = C_n^0 + C_n^1 + \cdots + C_n^{n-2} = (n-1)\cdot(n-1)!.$$

Da den algebraiske ligning af n^{te} grad

$$\omega_n(x) = C_n^0 x^n + C_n^1 x^{n-1} + \cdots + C_n^{n-1} x = 0,$$

hvor koefficienten til x^n er 1, har de n rødder

$$0, \ -1, \ -2, \ -3, \ \cdots, \ -(n-1),$$

og da de af disse rødder dannede potenssummer bliver

$$(-1)^p (1^p + 2^p + 3^p + \cdots + (n-1)^p) = (-1)^p S_p(n-1),$$

faas ved anvendelse af *Newtons* formler og efter en let omskrivning

$$(12)\quad p C_n^p = \sum_{r=1}^{r=p} (-1)^{r-1} C_n^{p-r} S_r(n-1), \qquad 1 \leqq p \leqq n-1.$$

Det er hidtil ikke lykkedes at vinde noget nærmere kendskab til de i de fem første eksempler definerede talteoretiske funktioner, naar n ikke er et helt tal. Den i eks. 6 nævnte funktion er et specielt tilfælde af gammafunktionen[1]) $\Gamma(x)$, idet man har $\Gamma(n+1) = n!$. Endvidere skal vi nu gaa over til at vise, at funktionerne $S_p(n)$ og C_n^p er hele polynomier i n.

---

43. Paa hvormange maader kan n deles i en sum af to uligestore addender, af hvilke ingen er 0?
44. Paa hvormange maader kan n skrives som et produkt af to uligestore faktorer, af hvilke ingen er 1?
45. Bevis formlerne
$$(S_1(n-1))^2 = S_2(n-1) + 2C_n^2.$$
46. Idet produkterne
$$F_n(x) = (1+x)\ (1+x^2) \cdot \cdots \cdot (1+x^n)$$
$$G_n(x) = (1+x^2)(1+x^4) \cdot \cdots \cdot (1+x^{2n})$$
$$H_n(x) = (1+x)\ (1+x^3) \cdot \cdots \cdot (1+x^{2n-1})$$
omskrives til hele polynomier i x, skal disses koefficienter defineres som talteoretiske funktioner af de tilsvarende eksponenter.
47. Hvilke relationer udledes mellem de i foregaaende opgave nævnte talteoretiske funktioner, hvis man anvender identiteten
$$F_{2n}(x) = G_n(x)\, H_n(x)?$$

§ 17. **Differensrækker af vilkaarlig orden.**

Betegner

$$(1)\quad f_r(x) = a_0 x^r + a_1 x^{r-1} + \cdots + a_{r-1} x + a_r$$

[1]) Se f. eks. min *Handbuch der Theorie der Gammafunktion;* Leipzig 1906.

et hvilketsomhelst helt polynomium af r^{te} grad, kaldes den af værdierne

(2) $$f_r(1),\ f_r(2),\ f_r(3),\ \cdots,\ f_r(n),\ \cdots$$

dannede talrække en differensrække af r^{te} orden; vi sætter

(3) $$F(n) = f_r(1) + f_r(2) + f_r(3) + \cdots + f_r(n).$$

For $r = 1$ danner tallene (2) en sædvanlig differensrække; denne er altsaa af første orden.

Under anvendelse af de i § 16 indførte potenssummer $S_p(n)$ findes umiddelbart af (1) og (3)

(4) $$F(n) = a_0 S_r(n) + a_1 S_{r-1}(n) + \cdots + a_{r-1} S_1(n) + n a_r.$$

Et andet udtryk for $F(n)$ kan findes, idet man benytter de ligeledes i § 16 indførte fakulteter. Det er nemlig muligt at skrive polynomiet $f_r(x)$ paa følgende form

(5) $$f_r(x) = \alpha_0 \omega_r(x) + \alpha_1 \omega_{r-1}(x) + \cdots + \alpha_{r-1} \omega_1(x) + \alpha_r,$$

hvor de enkelte koefficienter α_m, som man let ser, entydig kan bestemmes ved hjælp af de givne koefficienter a_p som homogene lineære funktioner med rationale koefficienter.

Sættes endvidere

(6) $$\Omega_p(n) = \omega_p(1) + \omega_p(2) + \cdots + \omega_p(n),$$

findes ved anvendelse af (3) og (5)

(7) $$F(n) = \alpha_0 \Omega_r(n) + \alpha_1 \Omega_{r-1}(n) + \cdots + \alpha_{r-1} \Omega_1(n) + n\alpha_r,$$

og det kommer saaledes an paa at summere den i (6) definerede specielle differensrække af p^{te} orden, altsaa at bestemme $\Omega_p(n)$.

I dette øjemed anvender vi identiteten

$$\omega_{p+1}(x+1) - \omega_{p+1}(x) = (p+1)\,\omega_p(x+1);$$

sættes dernæst $x+1$, $x+2$, $\cdots$, $x+n-1$ istedetfor x, og adderes alle disse ligninger, erholdes efter division med $p+1$

$$\omega_p(x+1) + \omega_p(x+2) + \cdots + \omega_p(x+n) = \frac{\omega_{p+1}(x+n) - \omega_{p+1}(x)}{p+1},$$

hvoraf for $x = 0$

$$(8)\quad \begin{cases} \Omega_p(n) = \dfrac{\omega_{p+1}(n)}{p+1} = \\ = \dfrac{1}{p+1}\left(C^0_{p+1}\, n^{p+1} + C^1_{p+1}\, n^p + \cdots + C^p_{p+1} n\right), \end{cases}$$

og altsaa findes ifølge (7) et udtryk af formen

$$(8)\qquad F(n) = \alpha'_0\, \omega_{r+1}(n) + \alpha'_1\, \omega_r(n) + \cdots + \alpha'_r\, \omega_1(n).$$

Erindres bestemmelsen af koefficienterne α_p i (5), og bemærkes det, at samtlige koefficienter i det i (8) angivne udtryk er rationale tal, faas den vigtige sætning:

I. *Den ved summen af de n første led i differensrækken af r^{te} orden i* (2) *definerede talteoretiske funktion $F(n)$ er et helt polynomium af $(r+1)^{\text{te}}$ grad i n:*

$$(10)\qquad F(n) = \beta_0\, n^{r+1} + \beta_1\, n^r + \cdots + \beta_{r-1}\, n^2 + \beta_r\, n;$$

dette polynomium indeholder intet af n uafhængigt led og er defineret i det af samtlige koefficienter i $f_r(x)$ dannede tallegeme.

Sættes specielt $f_r(x) = x^r$, faas følgende sætning, der skyldes *Pascal*[1]:

II. *Potenssummen*

$$S_p(n) = 1^p + 2^p + 3^p + \cdots + n^p$$

er et helt polynomium af $(p+1)^{\text{te}}$ grad i n; dette polynomium har lutter rationale koefficienter og indeholder intet led uafhængigt af n.

Anvendes dernæst formlen § 16, (12):

$$p\, C^p_n = \sum_{r=1}^{r=p} (-1)^{r-1}\, C^{p-r}_n\, S_r\,(n-1),$$

og erindres det, at

$$S_p(n-1) = S_p(n) - n^p,$$

faas ved anvendelse af II den ny sætning:

---

[1]) Traité sur la sommation des puissances numériques. Œuvres, Bd. III, p. 341—367; Paris 1908. Skriftet er sandsynligvis forfattet 1654.

III. *Holdes i fakultetkoefficienten C_n^p rangen p fast, er C_n^p et helt polynomium af graden $2p$ i n; dette polynomium har lutter rationale koefficienter og indeholder intet af n uafhængigt led.*

Af formlen § 16, (6) følger nemlig, at III gælder for C_n^1; det sædvanlige induktionsbevis fører derefter umiddelbart til maalet.

Medens vi i næste paragraf skal udtrykke koefficienterne i $S_p(n)$ ved bekendte rationale tal, frembyder koefficienterne i polynomiet for C_n^p større vanskeligheder [1]).

Eks. 1. Af identiteten

$$f_2(x) = ax^2 + bx + c = ax(x+1) + (b-a)x + c$$

faas ved anvendelse af (8) og (9)

$$f_2(1) + f_2(2) + f_2(3) + \cdots + f_2(n) = \\ = \frac{a}{3} n(n+1)(n+2) + \frac{b-a}{2} n(n+1) + cn,$$

hvoraf for $a = 1$, $b = c = 0$ den speciellere formel

$$(11) \quad 1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}.$$

---

48. Bestem polynomiet $f(x)$, naar

$$f(1) + f(2) + f(3) + \cdots + f(n) = n^3.$$

§ 18. Undersøgelse af potenssummerne $S_p(n)$.

Ifølge § 17, II haves et udtryk af formen

$$(1) \quad S_{p-1}(n) = 1^{p-1} + 2^{p-1} + 3^{p-1} + \cdots + n^{p-1} = \Phi_p(n),$$

hvor vi for kortheds skyld har sat

$$(2) \quad \Phi_p(x) = a_{p,0}x^p + a_{p,1}x^{p-1} + \cdots + a_{p,p-1}x, \quad \Phi_1(x) = x.$$

---

[1]) Se min afhandling: Recherches sur les polynomes et les nombres de Stirling. Annali di matematica (3) Bd. 10, p. 287—318; Milano 1904.

og hvor samtlige koefficienter $a_{p,r}$ er rationale tal. Ved en kombination af disse to formler, der altsaa udtrykker, at $\Phi_p(x)$ dels er et helt polynomium, dels en talteoretisk funktion, skal vi nu ad rent elementær vej udvikle elementerne af en teori for denne funktion; vi vil begynde med at bevise følgende sætninger:

I. *Betegner som sædvanlig C^r_{p-1} fakultetkoefficienterne af ordenen $p-1$, haves identiteten*:

$$(3)\quad \left\{ \begin{array}{l} C^0_{p-1}\,\Phi_p(x) + C^1_{p-1}\,\Phi_{p-1}(x) + \cdots + C^{p-2}_{p-1}\,\Phi_2(x) = \\ \qquad = \dfrac{x(x+1)\cdots(x+p-1)}{p} \end{array} \right.$$

Sættes nemlig i ligningen

$$y(y+1)\cdots(y+p-2) = C^0_{p-1}y^{p-1} + C^1_{p-1}y^{p-2} + \cdots + C^{p-2}_{p-1}y$$

efterhaanden $y = 1, 2, 3, \ldots, n$, og adderes alle de saaledes erholdte ligninger, faas ved anvendelse af summationsformlen § 17, (8) den for alle positive hele n gyldige ligning

$$(4)\quad \left\{ \begin{array}{l} C^0_{p-1}\,S_{p-1}(n) + C^1_{p-1}\,S_{p-2}(n) + \cdots + C^{p-2}_{p-1}\,S_1(n) = \\ \qquad = \dfrac{n(n+1)\cdots(n+p-1)}{p}; \end{array} \right.$$

hvis nu (3) ikke var identisk, maatte denne algebraiske ligning af p^{te} grad i x ifølge (4) have alle mulige positive hele tal til rødder, og det er umuligt.

Af (3) faas ved induktion følgende af *Pascal*[1]) fundne sætning:

II. *Koefficienterne i $\Phi_p(x)$ er saadanne rationale tal, at polynomiet $p!\,\Phi_p(x)$ har lutter hele talkoefficienter.*

Af (3) faas ligeledes ved induktion sætningen[2]):

---

[1]) Traité sur la sommation des puissances numériques. Œuvres, Bd. III, p. 341—397; Paris 1908.

[2]) Naar *Bachmann* i Encyklopädie der mathematischen Wissenschaften, Bd. I, p. 579, tilskriver *Lionnet* (Efter *Catalan* i Mém. de l'Acad. de Belgique, Bd. 46, p. 14; 1886) denne sætning, er dette næppe rigtigt.

III. *Betegner n et primtal, og antages $n \geqq p+1$, haves*

$$S_{p-1}(n) \equiv S_{p-1}(n-1) \equiv 0 \pmod{n}. \tag{5}$$

Sættes i formlen

$$(y+1)^p - y^p = \binom{p}{1} y^{p-1} + \binom{p}{2} y^{p-2} + \cdots + \binom{p}{p-1} y + 1$$

efterhaanden $y = 1, 2, 3, \cdots, n$, og adderes alle de saaledes erholdte ligninger, faas

$$(n+1)^p - 1 = \binom{p}{1} S_{p-1}(n) + \binom{p}{2} S_{p-2}(n) + \cdots + \binom{p}{p-1} S_1(n) + n,$$

hvoraf den ny sætning:

IV. *Polynomierne $\Phi_p(x)$ tilfredsstiller betingelserne*:

$$\begin{cases} (x+1)^p - 1 = \binom{p}{1} \Phi_p(x) + \binom{p}{2} \Phi_{p-1}(x) + \cdots \\ \qquad + \binom{p}{p-1} \Phi_2(x) + \Phi_1(x). \end{cases} \tag{6}$$

Sættes ligeledes i formlen

$$y^p(y+1)^p - y^p(y-1)^p = 2\left(\binom{p}{1} y^{2p-1} + \binom{p}{3} y^{2p-3} + \binom{p}{5} y^{2p-5} + \cdots\right),$$

der, for $p = 2q$ eller $p = 2q+1$, henholdsvis ender med leddet

$$\binom{2q}{2q-1} y^{2q+1}, \quad \binom{2q+1}{2q+1} y^{2q+1}, \tag{7}$$

efterhaanden $y = 1, 2, 3, \cdots, n$, og adderes alle disse resultater, faas den af *Stern*[1]) og *Lampe*[2]) fundne formel

---

[1]) Crelles Journal, Bd. 84, p. 216—218; 1878.

[2]) loc. cit. p. 270—272.

$$(8)\qquad \begin{cases} \frac{1}{2}n^p(n+1)^p = \\ = \binom{p}{1} S_{2p-1}(n) + \binom{p}{3} S_{2p-3}(n) + \binom{p}{5} S_{2p-5}(n) + \cdots, \end{cases}$$

hvoraf for $p = 2$ specielt

$$(9)\qquad 1^3 + 2^3 + \cdots + n^3 = \left(\frac{n(n+1)}{2}\right)^2 = (1+2+3+\cdots+n)^2.$$

Af (8) udledes paa sædvanlig maade sætningen:

V. *Polynomierne $\Phi_{2p}(x)$ med lige indices tilfredsstiller betingelserne*:

$$(10)\qquad \begin{cases} \frac{1}{2}x^p(x+1)^p = \\ = \binom{p}{1} \Phi_{2p}(x) + \binom{p}{3} \Phi_{2p-2}(x) + \binom{p}{5} \Phi_{2p-4}(x) + \cdots \end{cases}$$

Løses disse ligninger sukcessivt med hensyn til polynomierne $\Phi_{2p}(x)$, faas sætningen:

VI. *Polynomiet $\Phi_{2p}(x)$ med lige indeks er et helt polynomium af graden p i udtrykket $x(x+1)$; man finder:*

$$(11)\qquad \Phi_2(x) = \frac{x(x+1)}{2}$$

og almindelig for $p \geqq 2$:

$$(12)\qquad \begin{cases} \Phi_{2p}(x) = \alpha_{p,0}(x^2+x)^p + \alpha_{p,1}(x^2+x)^{p-1} + \cdots \\ \qquad + \alpha_{p,p-2}(x^2+x)^2; \end{cases}$$

$\Phi_{2p}(x)$ er saaledes for $p \geqq 2$ altid deleligt med $x^2(x+1)^2$.

Man finder f. eks.:

$$\Phi_2(x) = \tfrac{1}{2}x(x+1), \quad \Phi_4(x) = \tfrac{1}{4}x^2(x+1)^2$$
$$\Phi_6(x) = \tfrac{1}{6}x^3(x+1)^3 - \tfrac{1}{12}x^2(x+1)^2$$
$$\Phi_8(x) = \tfrac{1}{8}x^4(x+1)^4 - \tfrac{1}{6}x^3(x+1)^3 + \tfrac{1}{12}x^2(x+1)^2$$
$$\Phi_{10}(x) = \tfrac{1}{10}x^5(x+1)^5 - \tfrac{1}{4}x^4(x+1)^4 + \tfrac{3}{10}x^3(x+1)^3 - \tfrac{3}{20}x^2(x+1)^2.$$

Da udtrykket $x^2 + x$ bliver uforandret, naar x erstattes med $-x-1$, faas af (12) følgende sætning:

VII. *Polynomierne $\Phi_{2p}(x)$ med lige indices tilfredsstiller betingelsen*

$$(13)\qquad \Phi_{2p}(-x-1) = \Phi_{2p}(x).$$

Af de udviklede formler kan man uden vanskelighed udlede udtrykkene for de første af potenssummerne $S_p(n)$; allerede *Jacob Bernoulli*[1]) angav de 10 første af følgende bestemmelser af denne art:

$$S_1(n) = \frac{n^2}{2} + \frac{n}{2}$$

$$S_2(n) = \frac{n^3}{3} + \frac{n^2}{2} + \frac{n}{6}$$

$$S_3(n) = \frac{n^4}{4} + \frac{n^3}{2} + \frac{n^2}{4}$$

$$S_4(n) = \frac{n^5}{5} + \frac{n^4}{2} + \frac{n^3}{3} - \frac{n}{30}$$

$$S_5(n) = \frac{n^6}{6} + \frac{n^5}{2} + \frac{5n^4}{12} - \frac{n^2}{12}$$

$$S_6(n) = \frac{n^7}{7} + \frac{n^6}{2} + \frac{n^5}{2} - \frac{n^3}{6} + \frac{n}{42}$$

$$S_7(n) = \frac{n^8}{8} + \frac{n^7}{2} + \frac{7n^6}{12} - \frac{7n^4}{24} + \frac{n^2}{12}$$

$$S_8(n) = \frac{n^9}{9} + \frac{n^8}{2} + \frac{2n^7}{3} - \frac{7n^5}{15} + \frac{2n^3}{9} - \frac{n}{30}$$

$$S_9(n) = \frac{n^{10}}{10} + \frac{n^9}{2} + \frac{3n^8}{4} - \frac{7n^6}{10} + \frac{n^4}{2} - \frac{3n^2}{20}$$

$$S_{10}(n) = \frac{n^{11}}{11} + \frac{n^{10}}{2} + \frac{5n^9}{6} - n^7 + n^5 - \frac{n^3}{2} + \frac{5n}{66}$$

$$S_{11}(n) = \frac{n^{12}}{12} + \frac{n^{11}}{2} + \frac{11n^{10}}{12} - \frac{11n^8}{8} + \frac{11n^6}{6} - \frac{11n^4}{8} + \frac{5n^2}{12}.$$

---

49. Bevis formlen

$$S_p(1) + S_p(2) + \cdots + S_p(n) = (n+1)\,S_p(n) - S_{p+1}(n).$$

50. Bevis formlerne

$$2\,(S_3(n))^2 = S_7(n) + S_5(n),$$
$$5S_4(n) + S_2(n) = 6S_2(n) \cdot S_1(n),$$

der skyldes henholdsvis *Jacobi*[2]) og *Dostor*[3]).

---

[1]) Ars conjectandi, p. 97; Basel 1713.

[2]) Briefwechsel zwischen *Gauss* und *Schumacher*, Bd. V, p. 299; Altona 1863.

[3]) Nouvelles Annales (2) Bd. 18, p. 515—518; 1879.

51. Bevis formlerne, der skyldes *Dostor* [1]),

$$\frac{S_4(n) - S_2(n)}{S_3(n) - S_1(n)} = \tfrac{2}{5}(2n+1), \quad \frac{S_5(n) - S_3(n)}{S_3(n) - S_1(n)} = \tfrac{2}{3}n(n+1),$$

og angiv for hvilke former af n disse brøker bliver hele tal.

52. Bevis formlen

$$C_{p-1}^0 S_{p-1}(n) - C_{p-1}^1 S_{p-1}(n) + \cdots + (-1)^{p-2} C_{p-1}^{p-2} S_1(n) = \\ = \frac{(n+1)\,n\,(n-1)\cdot\cdots\cdot(n-p+2)}{p}.$$

53. Bevis, at, hvis n_1 og n_2 er indbyrdes primiske, positive hele tal, er

$$\frac{S_p(n_1 n_2)}{n_1 n_2} - \frac{S_p(n_1)}{n_1} - \frac{S_p(n_2)}{n_2}$$

for alle positive hele p et helt tal, og generaliser derpaa denne sætning ved indførelse af produktet $n_1 n_2 n_3 \cdots n_q$ [2]).

54. Bevis, at

$$\frac{S_{2p}(a^r)}{a^r} - \frac{S_{2p}(a^s)}{a^s}$$

altid er et helt tal.

55. Hvis $a_1, a_2, \ldots, a_r$ er samtlige primfaktorer i n, er

$$\frac{S_{2p}(n)}{n} - \sum_{s=1}^{s=r} \frac{S_{2p}(a_s)}{a_s}$$

et helt tal.

56. Er $p = 2n+1 > 3$ et primtal, og antages $1 \leqq q \leqq n-1$, haves

$$S_{2q}(n) \equiv 0 \pmod{p}.$$

§ 19. Videre undersøgelse af polynomiet $\Phi_p(x)$.

Af identiteten

$$S_{p-1}(n) - S_{p-1}(n-1) = n^{p-1}$$

faas umiddelbart sætningen:

---

[1]) loc. cit.

[2]) Opg. 53–55 efter *v. Staudt*; Crelles Journal, Bd. 21, p. 372–373 1840.

I. *Polynomiet* $\Phi_p(x)$ *tilfredsstiller differensligningen:*

$$\Phi_p(x) - \Phi_p(x-1) = x^{p-1}. \tag{1}$$

Ved hjælp af denne sætning kan man udlede rekursionsformler til bestemmelse af koefficienterne $a_{p,r}$ i polynomiet

$$\Phi_p(x) = a_{p,0}x^p + a_{p,1}x^{p-1} + \cdots + a_{p,p-1}x.$$

Søges nemlig i

$$\Phi_p(x-1) = a_{p,0}(x-1)^p + a_{p,1}(x-1)^{p-1} + \cdots + a_{p,r}(x-1)^{p-r} + \cdots + a_{p,p-1}(x-1)$$

koefficienten til x^{p-r}, bliver denne

$$a_{p,r}\binom{p-r}{0} - a_{p,r-1}\binom{p-r+1}{1} + \cdots + (-1)^r\binom{p}{r}a_{p,0};$$

indføres dette udtryk i (1), faas for $r = 1$

$$a_{p,0} = \frac{1}{p}, \tag{2}$$

medens man for $r > 1$ finder

$$\begin{cases} \binom{p-r+1}{1}a_{p,r-1} - \binom{p-r+2}{2}a_{p,r-2} + \cdots \\ \qquad + (-1)^{p-1}\binom{p}{r}a_{p,0} = 0. \end{cases} \tag{3}$$

Sættes dernæst almindelig

$$a_{p,r} = \frac{(p-1)!\,\alpha_r}{(p-r)!}, \quad \alpha_0 = 1, \tag{4}$$

antager (3) formen

$$\frac{\alpha_{r-1}}{1!} - \frac{\alpha_{r-2}}{2!} + \frac{\alpha_{r-3}}{3!} - \cdots + (-1)^{r-1}\frac{\alpha_0}{r!} = 0, \tag{5}$$

hvoraf det tydelig fremgaar, at tallene α_r samtlig er uafhængige af p og altsaa alene afhænger af r; efter denne bemærkning vil det nu være let at bevise formlerne

$$\alpha_{2r+1} = 0, \quad r \geqq 1. \tag{6}$$

Antages nemlig i (1) mærketallet lige, og erindres formlen § 18, (13),

$$\Phi_{2p}(x) = \Phi_{2p}(-x-1),$$

medens (1) giver

$$\Phi_{2p}(-x) = \Phi_{2p}(-x-1) - x^{2p-1},$$

findes umiddelbart

$$\Phi_{2p}(x) = \Phi_{2p}(-x) + x^{2p-1},$$

og altsaa haves for koefficienterne $a_{2p,\,2r+1}$:

$$a_{2p,1} = \tfrac{1}{2}; \quad a_{2p,\,2r+1} = 0, \quad r \geqq 1,$$

hvoraf (6) umiddelbart følger, fordi α_r er uafhængig af p.

For de ved ligningerne (5) bestemte tal α_r finder man for $r \geqq 1$

$$\alpha_{2r} = \frac{(-1)^{r-1} B_r}{(2r)!}, \tag{7}$$

hvor de positive, rationale tal B_r er de efter *Jacob Bernoulli* benævnte *Bernoulliske* tal[1]); disse tal synes første gang indførte i analysen gennem de i slutningen af foregaaende paragraf angivne udtryk for de første potenssummer $S_p(n)$.

Af (5) og (7) finder man for de første af tallene B_r

$$B_1 = \tfrac{1}{6}, \quad B_2 = \tfrac{1}{30}, \quad B_3 = \tfrac{1}{42}, \quad B_4 = \tfrac{1}{30}, \quad B_5 = \tfrac{5}{66}, \quad B_6 = \tfrac{691}{2730},$$

medens man for polynomiet $\Phi_p(x)$ umiddelbart finder det almindelige udtryk, gyldigt for $p \geqq 3$ [2]):

$$\Phi_p(x) = \frac{x^p}{p} + \frac{x^{p-1}}{2} + \sum_{r=1}^{\leqq \frac{p-1}{2}} \frac{(-1)^{r-1} B_r}{p} \binom{p}{2r} x^{p-2r}; \tag{8}$$

for $p = 2$ og $p = 1$ haves derimod henholdsvis

---

[1]) Se f. eks. min *Lærebog i elementær funktionsteori*, p. 359; 1909.

[2]) Fra et talteoretisk synspunkt er denne definition for de *Bernoulliske* funktioner den naturligste. I analysen tvinges man derimod til at indføre funktionen $\varphi_n(x)$ bestemt ved

$$\Phi_n(x) = (n-1)!\,\big(\varphi_n(x) - \varphi_n(0)\big), \quad \varphi'_n(x) = \varphi_{n-1}(x), \quad n \geqq 1.$$

Se min *Lærebog i elementær funktionsteori*, p. 402; 1909.

(9) $$\Phi_2(x) = \frac{x^2}{2} + \frac{x}{2}, \quad \Phi_1(x) = x.$$

Sættes i (1) $-x$ istedetfor x, og bemærkes det, at (8) og (9), for $p > 1$, umiddelbart giver

$$\Phi_p(-x) = (-1)^p \Phi_p(x) - (-1)^p x^{p-1},$$

faas følgende udvidelse af sætningen § 18, VII:

II. *Polynomiet* $\Phi_p(x)$ *tilfredsstiller, hvadenten* p *er lige eller ulige, betingelsen*

(10) $$\Phi_p(-x-1) = (-1)^p \Phi_p(x).$$

Af (1) og (8) faas endvidere sætningen:

III. *Antages* $p \geqq 2$, *dannes polynomiet* $\Phi_p(x-1)$ *af udtrykket for* $\Phi_p(x)$, *idet man blot skifter tegn for leddet med potensen* x^{p-1}:

(11) $$\begin{cases} \Phi_p(x-1) = \dfrac{x^p}{p} - \dfrac{x^{p-1}}{2} + \sum_{r=1}^{\leqq \frac{p-1}{2}} \dfrac{(-1)^{r-1} B_r}{p} \binom{p}{2r} x^{p-2r} \\ \Phi_2(x-1) = \dfrac{x^2}{2} - \dfrac{x}{2}. \end{cases}$$

Da man af (1) finder

(12) $$\Phi_p(-1) = \Phi_p(0) = 0, \quad p \geqq 2,$$

medens (10) for $x = -\frac{1}{2}$ giver

(13) $$\Phi_p(-\tfrac{1}{2}) = (-1)^p \Phi_p(-\tfrac{1}{2}); \quad \Phi_{2p+1}(-\tfrac{1}{2}) = 0, \quad p \geqq 1,$$

faas endvidere sætningen:

IV. *Antages* $p > 1$, *er polynomiet* $\Phi_{2p}(x)$ *med lige indeks deleligt med* $x^2(x+1)^2$, *medens* $\Phi_{2p+1}(x)$ *for* $p > 0$ *er deleligt med* $(2x+1)\,x(x+1)$.

Sættes, for $p \geqq 1$,

(14) $$\Phi_{2p+1}(x) = (2x+1)\,\Psi_{2p}(x),$$

faas ved anvendelse af (10)

(15) $$\Psi_{2p}(-x-1) = \Psi_{2p}(x),$$

og $\Psi_{2p}(x)$ kan følgelig skrives som et polynomium af p^{te} grad i størrelsen $x^2 + x$.

Paa denne maade findes udtryk af formen

$$(16)\quad \begin{cases} \Phi_{2p}(x) = \left(a_0(\Phi_2(x))^{p-2} + a_1(\Phi_2(x))^{p-3} + \cdots + a_{p-2}\right)\Phi_4(x) \\ \Phi_{2p+1}(x) = \left(b_0(\Phi_2(x))^{p-1} + b_1(\Phi_2(x))^{p-2} + \cdots + b_{p-1}\right)\Phi_3(x), \end{cases}$$

hvor man dog maa antage henholdsvis $p \geqq 2$ og $p \geqq 1$.

De af (16) for $p = 3$ erholdte specielle formler skyldes *Dostor*[1]), som aabenbart ikke kan have kendt de foran nævnte noter af *Stern* og *Lampe*.

Det i (8) fremstillede almindelige udtryk for $\Phi_p(x)$ er bl. a. angivne af *Cauchy*[2]) og *Raabe*[3]).

---

57. Det ved differensligningen

$$f(x) - f(x-1) = \alpha_0 x^{p-1} + \alpha_1 x^{p-2} + \cdots + \alpha_{p-2} x + \alpha_{p-1}$$

definerede hele polynomium $f(x)$ skal udvikles efter funktionerne $\Phi_p(x)$.

58. Sættes almindelig

$$\Phi_n(x) = F_n(x) + \tfrac{1}{2} x^{n-1},$$

skal man bevise formlen

$$(\Phi_n(x))^2 - (\Phi_n(x-1))^2 = 2x^{n-1} F_n(x)$$

og derefter udvikle $(\Phi_n(x))^2$ efter funktionerne $\Phi_p(x)$.

59. Produktet $\Phi_p(x)\,\Phi_q(x)$ skal udvikles efter polynomierne $\Phi_r(x)$.

60. Bevis, at den nødvendige og tilstrækkelige betingelse for at polynomiet af n^{te} grad

---

[1]) Archiv der Mathematik und Physik, Bd. 63, p. 439; 1879. Bd. 64, p. 315; 1879. Nouvelles Annales (2) Bd. 18, p. 515—518; 1879.

[2]) Résumés analytiques, p. 20; Turin 1833.

[3]) Die Jacob Bernoullische Function; Zürich 1848. Crelles Journal, Bd. 42, p. 348—376; 1851.

$$f(x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n$$

tilfredsstiller betingelsen $f(-x-1) = (-1)^n f(x)$, er, at

$$f(x) - f(x-1) = 2a_1 x^{n-1} + 2a_3 x^{n-3} + 2a_5 x^{n-5} + \cdots$$

61. Udtryk, med betegnelserne i foranstaaende opgave, koefficienterne a_{2p} ved $a_1, a_3, a_5, \ldots, a_{2p+1}$.

§ 20. **Nikomakos's regel. Liouvilles sætning.**

Af summationsformlen for den sædvanlige differensrække finder man umiddelbart

$$1) \qquad 1 + 3 + 5 + \cdots + (2n-1) = n^2,$$

hvorved ethvert kvadrattal altsaa kan opløses i en sum af paa hinanden følgende ulige tal, idet man stedse skal begynde med 1.

Nikomakos har angivet følgende regel til fremstilling af kubiktallene som summer af paa hinanden følgende ulige tal:

$$(2) \qquad \begin{cases} 1^3 = 1; \quad 2^3 = 3 + 5; \quad 3^3 = 7 + 9 + 11; \\ 4^3 = 13 + 15 + 17 + 19; \ \cdots \end{cases}$$

Denne regel kan generaliseres paa følgende maade:

I. *Er n og p positive hele tal, saaledes at $2p \leqq n$, haves for potensen a^n følgende fremstillinger som summer af paa hinanden følgende ulige tal:*

$$(3) \qquad a^n = \sum_{s=0}^{s=a^p-1} (a^{n-p} - a^p + 2s + 1).$$

Ved summation ser man umiddelbart, at differensrækken med differensen 2 og med a^p led, som indgaar i (3), har summen a^n, og det er indlysende, at tallet

$$a^{n-p} - a^p = a^p (a^{n-2p} - 1)$$

altid er et lige tal.

For $n = 2$ haves $p = 1$, og (3) giver som specielt tilfælde (1).

Antages $p = 1$, $n = 3$, ser man, at rækken, der fremstiller a^3, begynder med $a(a-1)+1$ og ender med $a(a+1)-1$, saa at $(a+1)^3$ maa begynde med det næste ulige tal $a(a+1)+1$. Man finder altsaa paa denne maade specielt et bevis for *Nikomakos's* regel.

Endvidere slutter man heraf, at summen af de n første kubiktal er summen af de $\frac{1}{2}n(n+1)$ første ulige tal og følgelig kvadratet paa summen af de n første tal i talrækken:

$$(4)\qquad \begin{cases} 1^3 + 2^3 + 3^3 + \cdots + n^3 = \left(\dfrac{n(n+1)}{2}\right)^2 = \\ \qquad = (1 + 2 + 3 + \cdots + n)^2. \end{cases}$$

Af den elementære formel (4) har *Liouville* [1]) udledt en mærkelig sætning; multipliceres nemlig de af (4) dannede ligninger

$$\begin{aligned} &\Sigma(1+\alpha_1)^3 = (\Sigma(1+\alpha_1))^2, \quad 0 \leqq \alpha_1 \leqq a_1, \\ &\Sigma(1+\alpha_2)^3 = (\Sigma(1+\alpha_2))^2, \quad 0 \leqq \alpha_2 \leqq a_2, \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ &\Sigma(1+\alpha_r)^3 = (\Sigma(1+\alpha_r))^2, \quad 0 \leqq \alpha_r \leqq a_r, \end{aligned}$$

faas umiddelbart

$$(5)\qquad \begin{cases} \Sigma((1+\alpha_1)(1+\alpha_2)\cdots(1+\alpha_r))^3 = \\ = (\Sigma(1+\alpha_1)(1+\alpha_2)\cdots(1+\alpha_r))^2, \end{cases}$$

hvor summationerne skal udstrækkes til de ovennævnte værdier af $\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_r$.

Betegner dernæst

$$d_1, d_2, d_3, \ldots, d_m, \quad m = \tau(n),$$

samtlige divisorer i tallet

$$n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r},$$

hvor $p_1, p_2, p_3, \ldots, p_r$ er forskellige primtal, haves for en vilkaarlig af divisorerne i (6) et udtryk af formen

$$d_s = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r},$$

---

[1]) Comptes rendus, Bd. 44, p. 753; 1857. Journal de Mathématiques (2) Bd. 2, p. 393–396; 1857.

hvor eksponenterne kan antage de ovennævnte værdier, og man finder

$$\tau(d_s) = (1 + \alpha_1)(1 + \alpha_2) \cdots (1 + \alpha_r);$$

indføres dette udtryk i (5), erholdes sætningen:

II. *Betegner* $d_1, d_2, d_3, \ldots, d_m$ *samtlige divisorer i et tal* n, *altsaa* $m = \tau(n)$, *haves*

$$\sum_{s=1}^{s=m} \left(\tau(d_s)\right)^3 = \left(\sum_{s=1}^{s=m} \tau(d_s)\right)^2.$$

---

62. Vis, at 9 er det eneste kvadrattal af formen $2^n + 1$.
63. Vis, at der ikke kan eksistere noget kubiktal af formen $2^n + 1$.
64. Vis, at summen af to paa hinanden følgende potenser af 8 enten er et kvadrattal eller det dobbelte af et kvadrattal.
65. Bestem to positive hele tal x og y, saaledes at summen af x paa hinanden følgende ulige tal, af hvilke det første er $2y + 1$, bliver et kvadrattal.
66. Bestem $2n + 1$ paa hinanden følgende kvadrater af positive hele tal, saaledes at summen af de $n + 1$ første er lig med summen af de øvrige[1]). Eks. $n = 1$, $n = 2$.

§ 21. Tal af specielle former.

Under talteoretiske funktioner har vi endnu tilbage at omtale visse tal af særlige former, der har spillet en vigtig rolle i den ældre tids elementære talteori. Af saadanne tal nævner vi følgende:

1⁰. *Polygonaltallene*, der for $n \geqq 3$ defineres som leddene i differensrækken af anden orden

(1) $\quad 1, n, 3n - 3, 6n - 8, \ldots, \frac{p(p-1)n}{2} - p(p-2), \ldots;$

[1]) *Tilly* har (Nouvelle correspondance mathématique, Bd. 5, p. 437—438; 1879) løst en almindeligere opgave. *Dostor* har (Archiv der Mathematik und Physik, Bd. 64, p. 350—352; 1880) givet en ret kompliceret løsning af vor speciellere opgave.

differenserne mellem to paa hinanden følgende af disse tal er altsaa leddene i differensrækken af første orden med differensen $n - 2$:

(2) $\quad n - 1,\ 2n - 3,\ 3n - 5,\ \ldots,\ (n-2)(p+1) + 1,\ \ldots.$

Af denne definition følger umiddelbart, at det r^{te} af tallene i (1), som vi betegner ved $P_{n,r}$, er summen af de $r - 1$ første led i rækken (2) forøget med 1; derved findes

$$(3) \qquad P_{n,r} = \frac{r(r-1)n}{2} - r(r-2).$$

Grunden til betegnelsen polygonaltal for tallene $P_{n,r}$ (n-kantstallene) ses let, idet man tegner regulære n-kanter, der er ligedan beliggende med en vinkelspids som fællespunkt, og hvis sider har længderne 1, 2, 3, ... Deles nemlig alle polygonsiderne med enheden, bliver antallet af de saaledes erholdte delingspunkter paa siderne i de r første polygoner netop tallet $P_{n,r}$.

Af (3) finder man for smaa værdier af r

$$(4) \quad \begin{cases} P_{3,r} = \dfrac{r(r+1)}{2}, & P_{4,r} = r^2, & P_{5,r} = \dfrac{r(3r-1)}{2} \\ P_{6,r} = r(2r-1), & P_{7,r} = \dfrac{r(5r-3)}{2}, & P_{8,r} = r(3r-2); \end{cases}$$

disse tal kaldes henholdsvis trigonal-, tetragonal-, pentagonal-, heksagonal, septagonal- og oktagonaltal.

Af (4) faas umiddelbart:

I. *Alle heksagonaltal er alle tetragonaltal af rangen* $2r - 1$, *medens alle pentagonaltal er tredjedelen af samtlige tetragonaltal af rangen* $3r - 1$.

Trigonaltallene er allerede betragtede af *pytagoræerne*; de spillede overhovedet en vigtig rolle for oldtidens matematikere; navnlig har *Diophant* undersøgt ikke blot disse tal, men polygonaltallene i det hele taget; han har saaledes angivet formlen

$$(5) \qquad 8(n-2)P_{n,r} + (n-4)^2 = ((n-2)(2r-1) + 2)^2.$$

For $n = 3$ faas heraf specielt for trigonaltallene

$$8P_{3,r} + 1 = 4r(r+1) + 1 = (2r+1)^2. \tag{6}$$

Diophant har ligeledes beskæftiget sig med ligningen

$$P_{n,r} = P_{m,q};$$

han angiver f. eks.

$$36 = P_{3,8} = P_{4,6} = P_{13,3} = P_{36,2}.$$

2°. *Polyedertallene* staar i lignende forhold til de *platoniske* legemer som polygontallene til de regulære polygoner; der eksisterer derfor fem klasser af disse tal, nemlig

tetraedertallene	af formen	$T_n = \frac{n(n+1)(n+2)}{6}$
heksaedertallene	» »	$H_n = n^3$
oktaedertallene	» »	$O_n = \frac{n(2n^2+1)}{3}$
dodekaedertallene	» »	$D_n = \frac{n}{2}(9n^2 - 9n + 2)$
ikosaedertallene	» »	$I_n = \frac{n}{2}(5n^2 - 5n + 2).$

3°. *Pyramidaltallene* $\Pi_{n,r}$ staar i samme forhold til de regulære pyramider som polygonaltallene til de regulære polygoner; man har derfor, idet $n \geqq 3$, bestandig

$$\Pi_{n,r} = P_{n,1} + P_{n,2} + \cdots + P_{n,r},$$

og altsaa findes ved (3) og § 17, (8) for $p = 2$

$$\Pi_{n,r} = \frac{(r-1)\,r\,(r+1)\,n}{6} - \frac{r(r+1)(2r-5)}{6},$$

hvoraf for $n = 4$ den bekendte formel for summen af de r første kvadrattal.

Polygonaltallene har spillet en ret vigtig rolle for *Fermat* ved hans banebrydende talteoretiske undersøgelser [1]).

---

[1]) Œuvres, Bd. II, p. 63. Se endvidere *Legendre:* Théorie des nombres, Bd. I, pp. 217--221, 393. Bd. II, p. 340—354. Zahlentheorie, Bd. I, pp. 218—221, 387. Bd. II, p. 332—348.

67. Bestem den almindelige form for to trigonaltal, hvis differens er et kvadrattal [1]).

68. Vis, at summen af de $2n$ første trigonaltal er det firdobbelte af summen af de n første kvadrattal.

69. Vis, at summen af de n første ulige kubiktal er et heksagonaltal [2]).

KAPITEL VI.

Fermats problem.

§ 22. Bemærkninger om kædebrøker.

Betegner

$$\frac{y_0}{z_0},\ \frac{y_1}{z_1},\ \frac{y_2}{z_2},\ \ldots,\ \frac{y_{n-1}}{z_{n-1}},\ \frac{y_n}{z_n}$$

konvergenterne i kædebrøken

$$K = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots + \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}}$$

eller som vi kortere skriver

$$(1) \qquad K = (a_0,\ a_1,\ a_2,\ \ldots,\ a_{n-1},\ a_n),$$

haves for $2 \leqq p \leqq n$ rekursionsformlerne [3])

$$(2) \qquad y_p = a_p y_{p-1} + y_{p-2},\quad z_p = a_p z_{p-1} + z_{p-2},$$

medens man for $1 \leqq p \leqq n$ bestandig har

$$(3) \qquad y_p z_{p-1} - z_p y_{p-1} = (-1)^{p-1}.$$

---

[1]) Sammenlign Nouvelles Annales (2) Bd. 17, p. 462—464; 1878.

[2]) *Lucas:* Théorie des nombres, Bd. I, p. 227; Paris 1891.

[3]) Se f. eks. min *Lærebog i kædebrøker og determinanter.* 1907.

Her vil vi udelukkende betragte saadanne kædebrøker, hvis ufuldstændige kvotienter $a_0, a_1, \ldots, a_n$ alle er positive hele tal. Antages da i (1) $a_n > 1$, kan vi ogsaa fremstille kædebrøken K paa formen

$$K = (a_0, a_1, a_2, \ldots, a_{n-1}, a_n - 1, 1), \tag{4}$$

medens man for $a_n = 1$ af (1) finder

$$K = (a_0, a_1, a_2, \ldots, a_{n-2}, a_{n-1} + 1). \tag{5}$$

Enhver kædebrøk med $n + 1$ ufuldstændige kvotienter kan derfor altid omformes til en anden kædebrøk, der enten har $n + 2$ eller n ufuldstændige kvotienter.

Vi erindrer om, hvorledes den positive, uægte og uforkortelige brøk $a : b$ ved anvendelse af den til tallene a og b svarende *Euklidiske* algoritme udvikles i kædebrøk med lutter positive hele ufuldstændige kvotienter:

$$\begin{aligned}
a &= a_0 b + r_0 \\
b &= a_1 r_0 + r_1 \\
r_0 &= a_2 r_1 + r_2 \\
&\cdots\cdots\cdots\cdots\cdots \\
r_{n-3} &= a_{n-1} r_{n-2} + 1 \\
r_{n-2} &= a_n;
\end{aligned}$$

ved denne algoritme findes

$$\frac{a}{b} = (a_0, a_1, a_2, \ldots, a_{n-1}, a_n). \tag{6}$$

Kræver man ydermere i (6) enten $a_n > 1$ eller $a_n = 1$, er denne kædebrøk entydig bestemt.

Betegner endvidere $p : q$ den næstsidste konvergent i kædebrøken (6), kan vi ifølge (4) og (5) skrive denne kædebrøk og derved bestemme p og q saaledes, at differensen paa venstre side i den af (3) dannede formel

$$aq - bp = \pm 1 \tag{7}$$

faar et ganske bestemt fortegn.

To kædebrøker K og K', der skrives med de samme ufuldstændige kvotienter, men i omvendt orden, kaldes mod-

satte kædebrøker. Er K den i (1) definerede, faas for den modsatte kædebrøk K':

$$K' = (a_n,\ a_{n-1},\ \ldots,\ a_1,\ a_0). \tag{8}$$

Om modsatte kædebrøker gælder sætningen:

I. *Har en kædebrøk K de to sidste konvergenter*

$$\frac{y_n}{z_n},\ \frac{y_{n-1}}{z_{n-1}}, \tag{9}$$

bliver de to sidste konvergenter i den modsatte kædebrøk K':

$$\frac{y_n}{y_{n-1}},\ \frac{z_n}{z_{n-1}}. \tag{10}$$

Da de til tallene y_n og y_{n-1}, z_n og z_{n-1} svarende *Euklidiske* algoritmer fremstilles ved rekursionsformlerne (2), og da de sidste ligninger i disse algoritmer henholdsvis bliver

$$\begin{aligned} y_1 &= a_1 y_0 + 1, & z_2 &= a_2 z_1 + 1, \\ y_0 &= a_0, & z_1 &= a_1, \end{aligned}$$

er vor sætning bevist.

Den i (1) definerede kædebrøk K kaldes symmetrisk, naar man for $0 \leqq p \leqq n$ bestandig har

$$a_p = a_{n-p}. \tag{11}$$

Da en symmetrisk kædebrøk er lig med sin modsatte kædebrøk, faas ved I umiddelbart sætningen:

II. *Den nødvendige og tilstrækkelige betingelse for, at en kædebrøk er symmetrisk, er, at dens to sidste konvergenter*

$$\frac{y_n}{z_n},\ \frac{y_{n-1}}{z_{n-1}}$$

tilfredsstiller betingelsen

$$z_n = y_{n-1}. \tag{12}$$

Af (3) og (12) faas for den symmetriske kædebrøk

$$y_n z_{n-1} - z_n^2 = (-1)^{n-1},\quad z_n^2 + (-1)^{n-1} \equiv 0 \pmod{y_n}, \tag{13}$$

og man beviser derefter uden vanskelighed sætningen:

III. *Den nødvendige og tilstrækkelige betingelse for, at den positive, uægte og uforkortelige brøk $a:b$ fremstilles ved en symmetrisk kædebrøk, er*

$$b^2 \pm 1 \equiv 0 \pmod{a}. \tag{14}$$

Ifølge (13) behøver vi kun at bevise, at betingelsen (14) er tilstrækkelig; udvikles $a:b$ i kædebrøk, og er den næstsidste konvergent $p:q$, kan vi ifølge bemærkningerne om formlen (7) vælge denne kædebrøk saaledes, at

$$aq - bp = \pm 1$$

har samme fortegn som det i (14) forhaanden værende. Erstattes kongruensen (14) med den tilsvarende ligning

$$ax - b^2 = \pm 1,$$

faas derfor ved subtraktion fra den foranstaaende

$$a(q - x) = b(p - b).$$

Da a og b er indbyrdes primiske, maa a gaa op i $p - b$, hvilket kun er muligt for $p = b$; ti, da $a > p$ og $a > b$, slutter man, at $|p - b| < a$. Ifølge II er den for $a:b$ fundne kædebrøk altsaa symmetrisk.

I læren om grænseværdier defineres, hvad vi skal forstaa ved værdien af en uendelig kædebrøk med lutter positive hele ufuldstændige kvotienter, og det vises, at enhver saadan kædebrøk fremstiller et ganske bestemt irrationalt tal, større end 1.

Det vises endvidere, at ethvert irrationalt tal, større end 1, altid paa en og kun paa en maade kan udvikles i en kædebrøk af denne art.

En uendelig kædebrøk kaldes periodisk, naar dens ufuldstændige kvotienter fra et vist mærketal at regne dannes af en bestemt samling tal, perioden, der stedse vender tilbage i samme orden.

En saadan kædebrøk kaldes rent periodisk, hvis den ikke indeholder andre ufuldstændige kvotienter end periodernes; ellers kaldes den blandet periodisk.

Bestaar perioden i en rent periodisk kædebrøk x af tallene

(15) $$\alpha_0,\ \alpha_1,\ \alpha_2,\ \ldots,\ \alpha_{n-1},\ \alpha_n,$$

sætter vi for kortheds skyld

(16) $$x = ((\alpha_0,\ \alpha_1,\ \alpha_2,\ \ldots,\ \alpha_{n-1},\ \alpha_n));$$

da x er et endeligt og bestemt tal, haves derfor

(17) $$x = (\alpha_0,\ \alpha_1,\ \alpha_2,\ \ldots,\ \alpha_{n-1},\ \alpha_n,\ x).$$

Har den blandet periodiske kædebrøk y perioden (15), og er de foran den første periode gaaende ufuldstændige kvotienter

(18) $$a_0,\ a_1,\ a_2,\ \ldots,\ a_{p-1},\ a_p,$$

sætter vi

(19) $$y = (a_0,\ a_1,\ \ldots,\ a_p,\ (\alpha_0,\ \alpha_1,\ \alpha_2,\ \ldots,\ \alpha_n));$$

ifølge (16) haves derfor

(20) $$y = (a_0,\ a_1,\ \ldots,\ a_{p-1},\ a_p,\ x).$$

---

70. Løs den ubestemte ligning $ax - by = c$, hvor a, b og c er hele tal, saaledes at a og b er indbyrdes primiske, ved at udvikle $a : b$ i kædebrøk [1]).

71. Tallene a_n og b_n defineres, saaledes at

$$a_0 = 1,\ a_1 = 2;\quad b_0 = 1,\ b_1 = 3,$$

medens man for $n \geqq 2$ bestandig har

$$a_n = 3a_{n-1} - a_{n-2},\ b_n = 3b_{n-1} - b_{n-2};$$

bevis formlerne

$$a_n a_{n-1} = b_{n-1}^2 + 1,\quad b_n b_{n-1} = a_n^2 - 1;$$
$$a_n a_{n-2} = a_{n-1}^2 + 1,\quad b_n b_{n-2} = b_{n-1}^2 - 1.$$

72. Med betegnelserne i opg. 71 skal man bestemme antallet af ufuldstændige kvotienter og den almindelige form for konvergenterne i de symmetriske kædebrøker, der fremstiller

$$\frac{b_n}{a_n},\ \frac{a_n}{b_{n-1}},\ \frac{a_n}{a_{n-1}},\ \frac{b_n}{b_{n-1}}.$$

---

[1]) *Lagrange* i Mémoires de l'Académie de Berlin 1767, p. 173—174 (1769).

§ 23. Lagranges sætning om periodiske kædebrøker.

Om uendelige, periodiske kædebrøker med lutter positive hele ufuldstændige kvotienter gælder to i talteorien fundamentale sætninger, der skyldes *Lagrange*[1]):

I. *Enhver periodisk kædebrøk med lutter positive hele ufuldstændige kvotienter er rod i en kvadratisk ligning med hele koefficienter.*

Er x en rent periodisk kædebrøk, og har den af perioden dannede kædebrøk

$$K = (\alpha_0, \alpha_1, \alpha_2, \ldots, \alpha_{n-1}, \alpha_n) \tag{1}$$

de to sidste konvergenter

$$\frac{y_n}{z_n}, \quad \frac{y_{n-1}}{z_{n-1}}$$

findes ved § 22, (17)

$$x = \frac{y_n x + y_{n-1}}{z_n x + z_{n-1}},$$

og altsaa er x den positive rod i den kvadratiske ligning med hele koefficienter

$$z_n x^2 - (y_n - z_{n-1}) x - y_{n-1} = 0. \tag{2}$$

For den blandet periodiske kædebrøk

$$y = (a_0, a_1, a_2, \ldots, a_k, (\alpha_0, \alpha_1, \alpha_2, \ldots, \alpha_n)), \tag{3}$$

hvor vi foreløbig antager $k \geqq 1$, betegner vi ved

$$\frac{\eta_k}{\xi_k}, \quad \frac{\eta_{k-1}}{\xi_{k-1}}$$

de to sidste konvergenter i den af de foran perioderne gaaende ufuldstændige kvotienter dannede kædebrøk

$$K_1 = (a_0, a_1, a_2, \ldots, a_{k-1}, a_k),$$

da findes ved (3)

---

[1]) Miscellanea Taurinensia, Bd. 4, p. 41—97; 1766—69. Mémoires de l'Académie de Berlin 1767.

$$y = \frac{\eta_k x + \eta_{k-1}}{\xi_k x + \xi_{k-1}}, \quad x = \frac{\eta_{k-1} - \xi_{k-1} y}{\xi_k y - \eta_k};$$

for $k = 0$ findes derimod

$$y = a_0 + \frac{1}{x}, \quad x = \frac{1}{y - a_0}.$$

Indsættes det saaledes fundne udtryk for x i ligningen (2), findes den kvadratiske ligning med hele koefficienter, hvori y er rod.

For at bevise den til I svarende omvendte sætning betragter vi en vilkaarlig kvadratisk ligning med rationale koefficienter og med reelle irrationale rødder. En saadan ligning kan altid bringes paa formen

$$Ax^2 + Bx + C = 0, \quad B^2 - 4AC > 0, \tag{4}$$

hvor A, B og C er hele tal, der ikke alle er delelige med et og samme hele tal større end 1, og hvor desuden $A > 0$.

Om ligningen (4) kan vi endvidere forudsætte, at den har mindst en positiv rod; ti var dette ikke tilfældet, havde ligningen

$$Ax^2 - Bx + C = 0$$

to positive rødder.

Vi kan endvidere forudsætte, at ligningen (4) med mindst en positiv rod har en rod større end 1; ti ellers vilde ligningen

$$\pm (Cx^2 + Bx + A) = 0$$

have denne egenskab.

Sættes i (4)

$$x = a + \frac{1}{x_1}, \tag{5}$$

faas for x_1 paany en kvadratisk ligning:

$$A_1 x_1^2 + B_1 x_1 + C_1 = 0, \tag{6}$$

hvor vi for kortheds skyld har sat

$$A_1 = Aa^2 + Ba + C, \quad B_1 = 2Aa + B, \quad C_1 = A, \tag{7}$$

og altsaa erholdes ved direkte udregning

$$B_1^2 - 4A_1 C_1 = B^2 - 4AC. \tag{8}$$

Antages den kvadratiske ligning (4) at have en positiv rod større end 1 og desuden en negativ rod, bliver denne ligning af formen

$$f(x) = Ax^2 + Bx - C = 0, \tag{9}$$

hvor A og C er positive hele tal. Vælges dernæst i (5) tallet a som det største positive hele tal, der er mindre end den positive rod i (9), bliver den til (6) svarende ligning af samme form som (9); ti

$$f(0) = -C$$

er negativ, og det samme maa derfor være tilfældet med

$$f(a) = Aa^2 + Ba - C;$$

den kontinuerte funktion $f(x)$ kan nemlig ikke skifte fortegn, naar x varierer mellem 0 og den positive rod i (9).

Antages den forelagte ligning (4) at have to positive rødder x og x', der begge er større end 1, og det saaledes, at x og x' begge falder mellem de samme to positive hele tal a_0 og $a_0 + 1$, sættes

$$x = a_0 + \frac{1}{x_1}, \quad x' = a_0 + \frac{1}{x'_1}, \quad x'_1 > x_1.$$

Har nu den for x_1 erholdte ligning

$$A_1 x_1^2 + B_1 x_1 + C_1 = 0$$

ligeledes sine to rødder x_1 og x'_1 beliggende mellem de samme to paa hinanden følgende positive hele tal a_1 og $a_1 + 1$, og sættes

$$x_1 = a_1 + \frac{1}{x_2}, \quad x'_1 = a_1 + \frac{1}{x'_2},$$

faas $x'_2 < x_2$, o. s. v.

Paa denne maade kan vi imidlertid ikke fortsætte ubegrænset; ti saa vilde de to rødder i (4) fremstilles ved samme uendelige kædebrøk med positive hele ufuldstændige kvotienter, og (4) maatte altsaa have et irrationalt tal som dobbeltrod, hvilket er umuligt.

Ved ovenstaaende fremgangsmaade maa vi derfor engang ende med en ligning af formen (9)

(9 a) $$Ax^2 + Bx - C = 0,$$

hvor A og C begge er positive hele tal, B derimod blot et helt tal; vi kan derfor ved vor følgende undersøgelse gaa ud fra (9 a).

For at udvikle den positive rod i (9) i kædebrøk skal vi altsaa bestemme de ufuldstændige kvotienter, idet vi efterhaanden sætter

$$x = a_0 + \frac{1}{x_1}, \quad x_1 = a_1 + \frac{1}{x_2}, \quad \ldots, \quad x_{n-1} = a_{n-1} + \frac{1}{x_n}; \quad \ldots;$$

de for størrelserne $x_1, x_2, x_3, \ldots, x_{n-1}, x_n, \ldots$ erholdte kvadratiske ligninger bliver ifølge vore bemærkninger om (9) alle af formen

(10) $$A_n x_n^2 + B_n x_n - C_n = 0,$$

hvor A_n og C_n er positive hele tal, og hvor vi ifølge (8) bestandig har

(11) $$B_n^2 + 4A_n C_n = B^2 + 4AC.$$

Da summen paa højre side i (11) er et fast positivt tal, slutter man heraf, at B_n kun kan have et begrænset antal forskellige værdier; ti kvadratet paa dette positive hele tal er altid mindre end $B^2 + 4AC$. Noget ganske lignende gælder øjensynlig begge de positive hele tal A_n og B_n. Ved fortsættelsen af vor operation maa vi derfor med visse mellemrum stedse genfinde en bestemt værdi B' for B_n.

Er de til B' svarende værdier af A_n og C_n henholdsvis

$$A'_1, A'_2, \ldots, A'_r,$$
$$C'_1, C'_2, \ldots, C'_r$$

saaledes at

$$B'^2 + 4A'_s C'_s = B^2 + 4AC, \quad 1 \leqq s \leqq r,$$

maa vi ligeledes med visse mellemrum finde kombinationen

$$B_n = B', \quad A_n = A'_s, \quad C_n = C'_s,$$

hvortil svarer den samme ligning af formen (10), og altsaa har vi bevist *Lagranges* omvending af 1:

II. *Enhver irrational rod, større end* 1, *i en kvadratisk ligning med rationale koefficienter kan udvikles i periodisk kædebrøk med lutter positive hele ufuldstændige kvotienter.*

Blandt de ved kædebrøksudviklingen dannede ligninger af formen (10) vælger vi den første, hvis rod fremstilles ved en rent periodisk kædebrøk; denne ligning er derfor altid af formen (2):

(2 a) $$z_n x^2 - (y_n - z_{n-1})\, x - y_{n-1} = 0;$$

sættes i (2 a) $x = -1 : x_1$, erholdes

$$y_{n-1} x_1^2 - (y_n - z_{n-1})\, x_1 - z_n + 0, \quad x_1 = \frac{y_n x_1 + z_n}{y_{n-1} x_1 + z_{n-1}}.$$

Den endelige kædebrøk, der dannes af perioden i den for x_1 erholdte uendelige kædebrøk, maa derfor ifølge § 22, I skrives med de samme cifre som perioden i x, blot er disse cifre tagne i omvendt orden.

---

73. Til hvilke grænseværdier konvergerer brøkerne i opg. 72, naar n vokser uden grænse?

74. Undersøg den uendelige kædebrøk

$$1 - \cfrac{1}{3 - \cfrac{1}{3 - \cfrac{1}{3 - \ddots}}},$$

§ 24. **Rent kvadratiske ligninger.**

For at undersøge de periodiske kædebrøker, der fremstiller irrationale reelle kvadratrødder af rationale tal, altsaa positive rødder i rent kvadratiske ligninger, vil vi nærmere betragte den blandet periodiske kædebrøk

(1) $$\xi = (a_0, a_1, a_2, \ldots, a_{k-1}, (\alpha_0, \alpha_1, \ldots, \alpha_{n-1})),$$

som forudsættes at have mindst to ufuldstændige kvotienter foran den første periode.

Vi sætter endvidere

$$x = ((\alpha_0,\ \alpha_1,\ \alpha_2,\ \ldots,\ \alpha_{n-1})), \tag{2}$$

og betegner ved

$$\frac{y_0}{z_0},\ \frac{y_1}{z_1},\ \ldots,\ \frac{y_{k-1}}{z_{k-1}},\ \ldots,\ \frac{y_{n+k-1}}{z_{n+k-1}}$$

konvergenterne i den endelige kædebrøk

$$(a_0,\ a_1,\ \ldots,\ a_{k-1},\ \alpha_0,\ \alpha_1,\ \ldots,\ \alpha_{n-1});$$

da haves for $k \geqq 3$

$$\begin{cases} y_{k-1} = a_{k-1} y_{k-2} + y_{k-3}, & z_{k-1} = a_{k-1} z_{k-2} + z_{k-3} \\ y_{n+k-1} = \alpha_{n-1} y_{n+k-2} + y_{n+k-3}, & z_{n+k-1} = \alpha_{n-1} z_{n+k-2} + z_{n+k-3}. \end{cases} \tag{3}$$

Endvidere finder man for $k \geqq 2$

$$\xi = \frac{y_{k-1} x + y_{k-2}}{z_{k-1} x + z_{k-2}} = \frac{y_{n+k-1} x + y_{n+k-2}}{z_{n+k-1} x + z_{n+k-2}},$$

eller, idet enhver af disse ligninger løses med hensyn til x:

$$x = \frac{y_{k-2} - z_{k-2}\,\xi}{z_{k-1}\,\xi - y_{k-1}} = \frac{y_{n+k-2} - z_{n+k-2}\,\xi}{z_{n+k-1}\,\xi - y_{n+k-1}}$$

hvoraf man let danner den kvadratiske ligning, hvis rod er ξ:

$$A\xi^2 + B\xi + C = 0; \tag{4}$$

man finder

$$A = z_{n+k-1} z_{k-2} - z_{n+k-2} z_{k-1}$$
$$B = z_{k-1} y_{n+k-2} + y_{k-1} z_{n+k-2} - z_{k-2} y_{n+k-1} - y_{k-2} z_{n+k-1}$$
$$C = y_{n+k-1} y_{k-2} - y_{n+k-2} y_{k-1}.$$

Antages her $k = 2$, findes

$$A = z_{n+1} - a_1 z_n = (\alpha_{n-1} - a_1)\, z_n + z_{n-1}$$
$$C = a_0 y_{n+1} - (a_0 a_1 + 1) y_n = a_0 y_n \left(\alpha_{n-1} - a_1 + \frac{y_{n-1}}{y_n} - \frac{1}{a_0}\right);$$

da nu $z_n > z_{n-1}$, $y_n > y_{n-1}$ og $a_0 \geqq 1$, ser man, at A og C maa have samme fortegn som det fra 0 forskellige hele tal $\alpha_{n-1} - a_1$. Havdes nemlig $\alpha_{n-1} = a_1$, gik der kun det ene ciffer a_0 foran den første periode.

Antages derimod $k \geqq 3$, faas ved anvendelse af (3), og efter en simpel omformning:

$$A = z_{k-2} z_{n+k-2} \left(\alpha_{n-1} - a_{k-1} + \frac{z_{n+k-3}}{z_{n+k-2}} - \frac{z_{k-3}}{z_{k-2}} \right)$$

$$C = y_{k-2} y_{n+k-2} \left(\alpha_{n-1} - a_{k-1} + \frac{y_{n+k-3}}{y_{n+k-2}} - \frac{y_{k-3}}{y_{k-2}} \right),$$

og altsaa har A og C samme fortegn som det fra 0 forskellige hele tal $\alpha_{n-1} - \alpha_{k-1}$; ti de to brudne tal i parenteserne paa højre side er ægte brøker.

Af disse bemærkninger faas umiddelbart sætningen:

I. *Har den blandet periodiske kædebrøk* ξ i (1) *mindst to ufuldstændige kvotienter foran den første periode, maa den anden rod i den kvadratiske ligning med rationale koefficienter, hvis ene rod er* ξ, *ligeledes være positiv.*

Denne sætning kan direkte anvendes paa den rent kvadratiske ligning

(5) $$x^2 - A = 0,$$

hvor $A > 1$ er et rationalt tal, som ikke er noget kvadrat.

Da den positive rod i (5) ifølge § 23, (2) ikke kan fremstilles ved nogen rent periodisk kædebrøk, haves ifølge I en udvikling af formen

(6) $$y = \sqrt{A} = (a, (\alpha_0, \alpha_1, \alpha_2, \ldots, \alpha_n));$$

antages her $n \geqq 1$, og betegner

$$\frac{y_0}{z_0}, \frac{y_1}{z_1}, \ldots, \frac{y_n}{z_n}$$

konvergenterne i den af en periode dannede kædebrøk, bliver

$$x = ((\alpha_0, \alpha_1, \alpha_1, \ldots, \alpha_n))$$

ifølge § 23, (2) rod i ligningen

$$z_n x^2 - (y_n - z_{n-1}) x - y_{n-1} = 0,$$

og denne ligning maa altsaa ved transformationen

$$y = a + \frac{1}{x}, \quad x = \frac{1}{y - a}$$

reduceres til en rent kvadratisk ligning i y.

Hertil kræves som nødvendig og tilstrækkelig betingelse

$$2ay_{n-1} = y_n - z_{n-1} = \alpha_n y_{n-1} + y_{n-2} - z_{n-1}$$

eller

$$(2a - \alpha_n) y_{n-1} = y_{n-2} - z_{n-1};$$

da $y_{n-1} > y_{n-2}$ og $y_{n-1} > z_{n-1}$, kan denne ligning da og kun da være mulig, naar

$$\alpha_n = 2a, \quad y_{n-2} = z_{n-1}.$$

Antages i (6) $n = 0$, er altsaa

$$\sqrt{A} = (a, (\alpha_0)),$$

bliver de tilsvarende ligninger

$$x^2 - \alpha_0 x - 1 = 0, \quad y^2 + (\alpha_0 - 2a) y + a^2 - \alpha_0 a - 1 = 0,$$

og altsaa haves $\alpha_0 = 2a$.

Erindres nu definitionen af tallene y_{n-2} og z_{n-1}, faas ved § 22, II følgende sætning:

II. *Den periodiske kædebrøk, som fremstiller det irrationale tal $\sqrt{A}$, hvor $A > 1$ er rational, er altid af formen*

(7) $$\sqrt{A} = (a, (\alpha_1, \alpha_2, \ldots, \alpha_{n-1}, 2a)), \quad \sqrt{A} = (a, (2a)),$$

hvor i første tilfælde den endelige kædebrøk

(8) $$(\alpha_1, \alpha_2, \ldots, \alpha_{n-1})$$

er symmetrisk.

Man ser umiddelbart, at kædebrøken i (7) ogsaa kan skrives paa formen

(9) $$y = (a, \alpha_1, \alpha_2, \ldots, \alpha_{n-1}, a + y), \quad y = (a, a + y),$$

og at en lignende formel gælder, hvis man istedetfor den ene periode medtager et vilkaarligt antal.

Betegner

(10) $$\frac{y_0}{z_0}, \frac{y_1}{z_1}, \frac{y_2}{z_2}, \ldots, \frac{y_m}{z_m}, \ldots$$

følgen af konvergenter i den i (7) angivne uendelige kædebrøk, og sættes, idet k er et vilkaarligt positivt helt tal,

(11) $$m = nk - 1,$$

haves almindelig den med (9) analoge formel

$$\sqrt{A} = \frac{(a + \sqrt{A})\, y_m + y_{m-1}}{(a + \sqrt{A})\, z_m + z_{m-1}}$$

eller

$$(az_m + z_{m-1})\sqrt{A} + Az_m = ay_m + y_{m-1} + y_m\sqrt{A},$$

hvoraf ifølge en bekendt sætning:

$$Az_m = ay_m + y_{m-1}$$
$$y_m = az_m + z_{m-1},$$

og altsaa erholdes ved elimination af a

$$y_m^2 - Az_m^2 = y_m z_{m-1} - z_m y_{m-1} = (-1)^{m-1},$$

hvoraf sætningen:

III. *De af konvergenterne* (10), *hvis mærketal er af formen* $nk - 1$, *hvis sidste ufuldstændige kvotient altsaa for* $n \geqq 1$ *stedse er tallet* a_{n-1}, *tilfredsstiller betingelsen*

(12) $$y_{nk-1}^2 - Az_{nk-1}^2 = (-1)^{nk}.$$

For den specielle kædebrøk $\sqrt{a^2 + 1} = (a, (2a))$ *faas derimod for alle* m

(13) $$y_m^2 - (a^2 + 1)\, z_m^2 = (-1)^{m+1}.$$

Er n et lige tal, bliver højre side i (12) stedse $+1$; for ulige n faar dette tal derimod værdien ± 1, eftersom k er lige eller ulige.

Eks. 1. Man finder

$$\sqrt{3} = (1, (1, 2));$$

konvergenterne er

$$\frac{1}{1},\ \frac{2}{1},\ \frac{5}{3},\ \frac{7}{4},\ \frac{19}{11},\ \frac{26}{15},\ \frac{71}{41},\ \frac{97}{56},\ \cdots;$$

for hveranden af disse konvergenters tællere og nævnere findes

$$1 = 2^2 - 3\cdot 1^2 = 7^2 - 3\cdot 4^2 = 26^2 - 3\cdot 15^2 = 97^2 - 3\cdot 56^2 = \cdots.$$

Eks. 2. For kædebrøken

$$\sqrt{2} = (1, (2))$$

med konvergenterne

$$\frac{1}{1}, \frac{3}{2}, \frac{7}{5}, \frac{17}{12}, \frac{41}{29}, \frac{99}{70}, \frac{239}{169}, \ldots$$

findes

$$-1 = 1^2 - 2 \cdot 1^2 = 7^2 - 2 \cdot 5^2 = 41^2 - 2 \cdot 29^2 = 239^2 - 2 \cdot 169^2 = \ldots$$
$$1 = 3^2 - 2 \cdot 2^2 = 17^2 - 2 \cdot 12^2 = 99^2 - 2 \cdot 70^2 = \ldots$$

§ 25. Lagranges løsning af Fermats problem.

I et til *Frénicle* adresseret brev af 1657 stillede *Fermat*[1]) følgende sætning som opgave:

Hvis det positive hele tal a ikke er et kvadrattal, eksisterer der uendelig mange positive hele tal y, saaledes at $ay^2 + 1$ *er et kvadrat.*

Det første hidtil kendte forsøg paa at bevise denne sætning skyldes *William Brouncker*; hans bevis, der er redigeret af *John Wallis*[2]) og senere anvendt af *Euler*[3]), er meget kompliceret og noget mangelfuldt; ti det viser ikke i alle tilfælde, at den stillede opgave virkelig har uendelig mange løsninger.

Det er først *Lagrange*[4]), som ved anvendelse af sin formel § 24, (12) har givet et ligesaa elegant som eksakt bevis.

Betegnes i kædebrøken

$$(1) \qquad \sqrt{a} = (\alpha, (\alpha_1, \alpha_2, \ldots, \alpha_{k-1}, 2\alpha)), \quad \sqrt{a} = (\alpha, (2\alpha))$$

konvergenterne ved

$$(2) \qquad \frac{y_0}{z_0}, \frac{y_1}{z_1}, \ldots, \frac{y_{k-1}}{z_{k-1}}, \frac{y_k}{z_k}, \ldots,$$

og sættes for alle positive hele n

[1]) Varia opera mathematica, p. 190; Toulouse 1679. Œuvres, Bd. II, p. 333.

[2]) Commercium epistolicum; London 1658.

[3]) Algebra, Bd. II, 2, Kap. VII. St. Petersborg 1771. 3. udg. Berlin 1821. Fransk udgave af *Lagrange*, 1795.

[4]) Miscellanea Taurinensia, Bd. 4, p. 41—47; 1766—69. Mémoires de l'Académie de Berlin 1767, p. 165—230; (1769). *Lagrange* behandler den almindeligere ligning $x^2 - ay^2 = b$.

(3) $$A_n = y_{nk-1}, \quad B_k = z_{nk-1},$$

haves ifølge § 24, (12), for alle n

(4) $$A_n^2 - aB_n^2 = (-1)^{nk} = \varepsilon_n,$$

hvorefter man uden vanskelighed beviser sætningerne:

I. *Har den for $\sqrt{a}$ erholdte periodiske kædebrøk et lige antal ufuldstændige kvotienter i perioden, tilfredsstilles ligningen*

(5) $$x^2 - ay^2 = 1$$

af alle tal af formen $x = A_n$, $y = B_n$, men ikke af andre positive hele tal, og ligningen

(6) $$x^2 - ay^2 = -1$$

har ingen heltallige løsninger.

II. *Indeholder kædebrøken for $\sqrt{a}$ et ulige antal ufuldstændige kvotienter, tilfredsstilles ligningerne*

(7) $$x^2 - ay^2 = 1, \quad x^2 - ay^2 = -1$$

af henholdsvis

(8) $$x = A_{2n},\ y = B_{2n}; \quad x = A_{2n+1},\ y = B_{2n+1},$$

men ikke af andre positive hele tal.

I henhold til (4) behøver vi kun at bevise, at der ikke findes andre løsninger end de ovenfor angivne.

Antages, at

(9) $$x^2 - ay^2 = \pm 1,$$

og antages endvidere foreløbig $y > 1$, har kædebrøken

$$\frac{x}{y} = (\alpha,\ \alpha_1,\ \alpha_2,\ \ldots,\ \alpha_{p-1})$$

mindst to ufuldstændige kvotienter; ti x og y er indbyrdes primiske; altsaa eksisterer kædebrøken

(10) $$\frac{x_1}{y_1} = (\alpha_1,\ \alpha_2,\ \ldots,\ \alpha_{p-1}),$$

og man har

$$\frac{x}{y} = \alpha + \frac{y_1}{x_1} = \frac{\alpha x_1 + y_1}{x_1}.$$

Heraf findes atter

(11) $$x = \alpha x_1 + y_1, \quad y = x_1;$$

ti begge brøkerne i ovenstaaende ligning er uforkortelige.

Af (9) og (11) erholdes imidlertid

$$(\alpha x_1 + y_1)^2 - a x_1^2 = \pm 1; \quad (a - \alpha^2) x_1^2 - 2\alpha x_1 y_1 = y_1^2 \mp 1,$$

hvilket giver

$$y_1^2 \mp 1 \equiv 0 \pmod{x_1},$$

saa at kædebrøken i (10) ifølge § 22, III er symmetrisk; sættes dernæst

$$\sqrt{b} = (\alpha, (\alpha_1, \alpha_2, \ldots, \alpha_{p-1}, 2\alpha)),$$

haves ifølge § 24, (12)

(12) $$x^2 - by^2 = \pm 1.$$

Er nu tegnene i (9) og (12) de samme, erholdes

$$(a - b) y^2 = 0, \quad a = b;$$

er disse fortegn derimod ikke ens, finder man

$$(a - b) y^2 = \pm 2,$$

hvilket er umuligt, fordi 2 ikke kan være deleligt med kvadrattallet $y^2 > 1$. Hermed er vore sætninger beviste for $y > 1$.

Antages $y = 1$, gives der kun følgende to muligheder

(13) $$a = c^2 + 1, \quad a = c^2 - 1;$$

i disse tilfælde finder man uden vanskelighed

$$\sqrt{c^2 + 1} = (c, (2c)), \quad \sqrt{c^2 - 1} = (c - 1, (1, 2c - 2));$$

de første konvergenter bliver henholdsvis

$$\frac{c}{1}, \frac{2c^2 + 1}{2c}; \quad \frac{c - 1}{1}, \frac{c}{1}, \frac{2c^2 - c - 1}{2c - 1},$$

og vore sætninger er altsaa fuldstændig beviste.

Om de saaledes fundne eneste mulige løsninger (A_n og B_n) af ligningen (5) eller af systemet (7) vil vi dernæst bevise sætningen[1]):

III. *Betegner n og p hvilkesomhelst positive hele tal, haves stedse*

$$\begin{cases} A_{n+p} = A_p A_n + aB_p B_n \\ B_{n+p} = B_p A_n + A_p B_n, \end{cases} \tag{14}$$

og derved findes

$$(A_1 \pm B_1\sqrt{a})^n = A_n \pm B_n\sqrt{a}. \tag{15}$$

Ifølge (13) kan vi indskrænke os til at bevise (14) for saadanne n, der tilfredsstiller betingelsen $nk \geqq 2$.

Sættes da i henhold til (3)

$$y_{nk-2} = a_n, \quad z_{nk-2} = b_n,$$

faar kædebrøken, der dannes af (1) ved til konvergenten med indeks $nk - 1$ at føje endnu den ufuldstændige kvotient α, værdien

$$\frac{\alpha y_{nk-1} + y_{nk-2}}{\alpha z_{nk-1} + z_{nk-2}} = \frac{\alpha A_n + a_n}{\alpha B_n + b_n},$$

og da denne kædebrøk er symmetrisk, faas ifølge § 22, II

$$A_n = \alpha B_n + b_n. \tag{16}$$

Endvidere finder man med disse betegnelser:

$$\begin{aligned} y_{nk} &= 2\alpha A_n + a_n = \alpha A_n + (\alpha A_n + a_n) \\ z_{nk} &= 2\alpha B_n + b_n = \alpha B_n + A_n, \end{aligned}$$

hvoraf:

$$\begin{aligned} y_{nk+1} &= \alpha_1 y_{nk} + A_n = (\alpha\alpha_1 + 1) A_n + \alpha_1 (\alpha A_n + a_n) \\ z_{nk+1} &= \alpha_1 z_{nk} + B_n = (\alpha\alpha_1 + 1) B_n + \alpha_1 A_n \end{aligned}$$

eller i henhold til definitionerne (2)

$$\begin{aligned} y_{nk+1} &= y_1 A_n + z_1 (\alpha A_n + a_n) \\ z_{nk+1} &= y_1 B_n + z_1 A_n; \end{aligned}$$

ved induktion findes dernæst almindelig

[1]) Formlerne (14) og (15) findes hos *Lagrange* i Mémoires de l'Académie de Berlin 1767, pp. 174—176, 226, 229; (1769).

Sættes i formlerne (side 74) $A = a$ $m = nk-1$, bliver disse formler

$$a z_{nk-1} = \alpha y_{nk-1} + y_{nk-2}, \quad y_{nk-1} = \alpha z_{nk-1} + z_{nk-2},$$

og derefter findes:

$$\begin{aligned} y_{nk} &= 2\alpha y_{nk-1} + y_{nk-2} = \alpha y_{nk-1} + a z_{nk-1} \\ z_{nk} &= 2\alpha z_{nk-1} + z_{nk-2} = \alpha z_{nk-1} + y_{nk-1}. \end{aligned}$$

Disse formler kan ogsaa skrives som

$$\begin{aligned} y_{nk} &= y_0 y_{nk-1} + a z_0 z_{nk-1} \\ z_{nk} &= y_0 z_{nk-1} + z_0 y_{nk-1}; \end{aligned}$$

ved induktion faas da almindelig

$$\begin{aligned} y_{nk+r} &= y_r y_{nk+1} + a z_r z_{nk+r-1} \\ z_{nk+r} &= y_r z_{nk-1} + z_r y_{nk-1}. \end{aligned}$$

Antages specielt $r = pk-1$, faas af disse formler

$$\begin{aligned} A_{n+p} &= A_n A_p + a B_n B_p \\ B_{n+p} &= A_n B_p + B_n A_p. \end{aligned}$$

Tallene w_r bestemt ved ligningerne

$$y_r^2 - a z_r^2 = (-1)^{r-1} w_r$$

er alle positive, fordi $\sqrt{a}$ er større end alle konvergenterne med lige nævnertal, men mindre end dem med ulige.

Da ovenstaaende formler ogsaa kan skrives som

$$\begin{aligned} y_{nk+r} &= A_n y_r + a B_n z_r \\ z_{nk+r} &= A_n z_r + B_n y_r, \end{aligned}$$

faas ved multiplikation

$$y_{nk+r}^2 - a z_{nk+r}^2 = (A_n^2 - a B_n^2)(y_r^2 - a z_r^2) = (-1)^{nk+r-1} w_r$$

og altsaa kaldes

$$w_{nk+r} = w_r$$

saaledes at disse tal kommer periodisk, og man behøver derfor kun at kende

$$\omega_0 \; \omega_1 \; \ldots \; \omega_{k-2}$$

og denne samling er tilmed periodisk, hvilket umiddelbart indses ved at multipliere de to ligninger

$$A_1^2 - a B_1^2 = (-1)^{k-1}$$
$$y_r^2 - a z_r^2 = (-1)^{r-1} \omega_r;$$

derved faas nemlig

$$(A_1 y_r - a B_1 z_r)^2 - a (A_1 z_r - B_1 y_r)^2 = (-1)^{k+r} \omega_r.$$

Er a en vilkaarlig ulige potens af et vilkaarligt ulige primtal p, haves $p^{2n} = 8k+1$, saaledes at a og p giver samme rest modulo 8.

Den ubestemte ligning

(1) $\quad x^2 - ay^2 = 1$

kan altid løses i hele tal; 6 vingesdenne ligning paa formen

(2) $\quad (x+1)(x-1) = ay^2;$

og bemærkes det, at faktorerne $x+1$ og $x-1$ enten er indbyrdes primiske eller har største fælles faktor 2, faas

(3) $\quad x \pm 1 \equiv 0 \pmod{a}.$

Antages først x ulige, faas af (3)

(4) $\quad x \pm 1 = 2u^2 \quad x \mp 1 = 2av^2,$

hvor u og v er indbyrdes primiske, og hvor $y = u \cdot v$; af (4) findes umiddelbart

(5) $\quad u^2 - av^2 = \pm 1,$

hvor tegnene i (4) og (5) er sammenhørende.

Er nu x og y de mindste positive hele tal, der tilfreds-

$$y_{nk+r} = y_r A_n + z_r (\alpha A_n + a_n)$$
$$z_{nk+r} = y_r B_n + z_r A_n,$$

hvoraf specielt for $r = k - 1$

$$(17) \qquad \begin{cases} A_{n+1} = A_1 A_n + B_1 (\alpha A_n + a_n) \\ B_{n+1} = A_1 B_n + B_1 A_n. \end{cases}$$

Af identiteterne

$$(A_1 + B_1 \sqrt{a})(A_n + B_n \sqrt{a}) = A_1 A_n + a B_1 B_n + B_{n+1} \sqrt{a}$$
$$(A_1 - B_1 \sqrt{a})(A_n - B_n \sqrt{a}) = A_1 A_n + a B_2 B_n - B_{n+1} \sqrt{a}$$

findes derpaa ved multiplikation og anvendelse af (4)

$$(A_1 A_n + a B_1 B_n)^2 - a B_{n+1}^2 = \varepsilon_1 \varepsilon_n = \varepsilon_{n+1},$$

og altsaa haves ved anvendelse af den første (17)

$$(18) \qquad A_{n+1} = A_1 A_n + a B_1 B_n; \quad a B_n = \alpha A_n + a_n.$$

Ved (16) findes derefter

$$(19) \qquad \frac{\alpha y_{nk-1} + y_{nk-2}}{\alpha z_{nk-1} + z_{nk-2}} = \frac{\alpha A_n + a_n}{\alpha B_n + b_n} = \frac{a B_n}{A_n}.$$

Formlerne (14) er saaledes beviste for alle n og $p = 1$; sættes i (17) og (18) $n = 1, 2, 3, \ldots$, bevises de almindelige formler (14) let ved induktion.

Da dernæst formlen (15) gælder for $n = 1$, og da vi ved multiplikation af (15) med de tilsvarende udtryk for $n = 1$ netop genfinder (17) og (18) bevises (15) ogsaa umiddelbart ved induktion.

Udvikles venstre side i (15) efter binomialformlen, faas A_n og B_n for ethvert n direkte udtrykt ved A_1, B_1 og a.

Medens vi saaledes fuldstændig behersker ligningen

$$x^2 - ay^2 = 1,$$

er vi trods indgaaende undersøgelser af *Legendre*[1]), *Lejeune Dirichlet*[2]) og andre endnu ikke istand til at angive, hvilke betingelser a skal opfylde, for at den tilsvarende ligning

[1]) Théorie des nombres, Bd. I, p. 64—71. Zahlentheorie, Bd. I, p. 64—73.
[2]) Abhandlungen der Berliner Akademie 1834, p. 649—664. Werke, Bd. I, p. 221—236.

$$x^2 - ay^2 = -1$$

kan løses i hele tal.

Carl Ferdinand Degen[1]) har forøvrig beregnet tabeller over de mindste værdisæt for x og y svarende til $x^2 - ay^2 = 1$ for $1 \leqq a \leqq 1000$ og tilsvarende værdisæt for saadanne $a < 1000$, for hvilke $x^2 - ay^2 = -1$ har løsninger.

Naar den førstnævnte af disse ligninger hyppig kaldes den *Pellske* ligning, skyldes dette en lapsus memoriæ af *Euler*[2]); *Pell* har intet selvstændigt bidrag givet til udviklingen af denne lignings teori[3]).

Den i sætningen I angivne metode kendtes allerede af inderne, og *Euklid* har beskæftiget sig med $x^2 - 2y^2 = \pm 1$.

De nævnte to ligninger $x^2 - ay^2 = \pm 1$ frembyder desuden andre ejendommelige modsætninger, som vi her kort vil omtale.

Betegner p et hvilketsomhelst helt tal, kan ligningen

$$x^2 - ap^2y^2 = 1$$

ligeledes løses i hele tal; vi er altsaa her istand til at angive saadanne n, at B_n bliver delelig med p. Noget tilsvarende gælder derimod ikke almindelig om $x^2 - ay^2 = -1$.

J. Perrott[4]) har undersøgt ligningen

$$x^2 - 2p^2y^2 = -1,$$

hvor p er et primtal af formen $4m + 1$, og vist, at denne ligning f. eks. ikke har hele løsninger for $p = 353$. Der gives altsaa for $a = 2$ intet B_{2n+1}, som er deleligt med 353.

---

75. Vis, at med de ovenstaaende almindelige betegnelser er B_n altid delelig med B_p, naar n er delelig med p, og omvendt.

---

[1]) Canon Pellianus sive tabula simplicissimam æquationis celebratissimæ: $y^2 = ax^2 + 1$ solutionem, pro singulis numeri dati valoribus ab 1 usque ad 1000, in numeris rationalibus iisdemque integris exhibens; København 1817.

[2]) Algebra, Bd. II, Kap. VII, § 98.

[3]) *Pell* har dog gengivet *Brounckers* løsning i *Rhonius's* algebra translated by *Th. Branker*, much altered and augmented; London 1668.

[4]) Crelles Journal, Bd. 102, p. 185–223; 1888.

stiller (1), kan værdien +1 i (5) ikke benyttes, og denne ligning bliver

(6) $u^2 - av^2 = -1$.

Da −1 er ikkerest for alle primtal af formen $4k+3$, maa a og dermed p altsaa være af formen $4k+1$, saaledes at (6) altid kan løses i dette tilfælde.

Da endvidere −1 er ikkerest for 4, maa, i (6), u være lige, v ulige.

Betegner

(7) $u = A_n$, $v = B_n$, $n = 1, 2, 3, \ldots$

løsningerne af (6), har Lagrange vist, hvorledes alle disse løsninger bestemmes ved hjælp af konvergenterne i kædebrøken, der fremstiller $\sqrt{a}$.

Er A_1 og B_1 bestemt, findes de følgende løsninger ved hjælp af Lagranges rekursionsformler

(8) $A_{n+p} = A_n A_p + a B_n B_p$, $B_{n+p} = A_n B_p + A_p B_n$,

hvor, for alle m,

(9) $A_m^2 - a B_m^2 = (-1)^m$.

Antages i den sidste (8) $p = n$, faas $B_{2n} = 2 A_n B_n$, saaledes at B_{2n} altid er lige, A_{2n} følgelig ulige; da nu tegnene i (4) og (5) er sammenhørende, bliver ~~den sidste~~ kongruensen (3), ifølge den sidste (2), altsaa i dette tilfælde

(10) $A_{2n} - (-1)^n \equiv 0 \pmod{a}$.

Som anvendelse vil vi bevise, at enhver af de ubestemte ligninger

(11) $ax^2 \pm 2x = y^2$

kan løses i hele tal og bestemme disse løsninger.

Multipliceres (11) med a, faas

$$(ax \pm 1)^2 - ay^2 = 1,$$

og altsaa haves, ifølge (10) for det øverste fortegn

(12) $x = \dfrac{A_{4n} - 1}{a}$, $y = B_{4n}$,

medens det nederste fortegn giver

$$x^2 - ay^2 = -1$$

kan løses i hele tal.

Carl Ferdinand Degen[1]) har forøvrig beregnet tabeller over de mindste værdisæt for x og y svarende til $x^2 - ay^2 = 1$ for $1 \leqq a \leqq 1000$ og tilsvarende værdisæt for saadanne $a < 1000$, for hvilke $x^2 - ay^2 = -1$ har løsninger.

Naar den førstnævnte af disse ligninger hyppig kaldes den *Pellske* ligning, skyldes dette en lapsus memoriæ af *Euler*[2]); *Pell* har intet selvstændigt bidrag givet til udviklingen af denne lignings teori[3]).

Den i sætningen I angivne metode kendtes allerede af inderne, og *Euklid* har beskæftiget sig med $x^2 - 2y^2 = \pm 1$.

De nævnte to ligninger $x^2 - ay^2 = \pm 1$ frembyder desuden andre ejendommelige modsætninger, som vi her kort vil omtale.

Betegner p et hvilketsomhelst helt tal, kan ligningen

$$x^2 - ap^2y^2 = 1$$

ligeledes løses i hele tal; vi er altsaa her istand til at angive saadanne n, at B_n bliver delelig med p. Noget tilsvarende gælder derimod ikke almindelig om $x^2 - ay^2 = -1$.

J. Perrott[4]) har undersøgt ligningen

$$x^2 - 2p^2y^2 = -1,$$

hvor p er et primtal af formen $4m + 1$, og vist, at denne ligning f. eks. ikke har hele løsninger for $p = 353$. Der gives altsaa for $a = 2$ intet B_{2n+1}, som er deleligt med 353.

---

75. Vis, at med de ovenstaaende almindelige betegnelser er B_n altid delelig med B_p, naar n er delelig med p, og omvendt.

---

[1]) Canon Pellianus sive tabula simplicissimam æquationis celebratissimæ: $y^2 = ax^2 + 1$ solutionem, pro singulis numeri dati valoribus ab 1 usque ad 1000, in numeris rationalibus iisdemque integris exhibens; København 1817.

[2]) Algebra, Bd. II, Kap. VII, § 98.

[3]) *Pell* har dog gengivet *Brounckers* løsning i *Rhonius's* algebra translated by *Th. Branker*, much altered and augmented; London 1668.

[4]) Crelles Journal, Bd. 102, p. 185–223; 1888.

Stiller (1), kan værdien +1 i (5) ikke benyttes, og denne ligning bliver

(6) $u^2 - av^2 = -1$.

Da -1 er ikkerest for alle primtal af formen $4k+3$, maa a og dermed p altsaa være af formen $4k+1$, saaledes at (6) altid kan løses i dette tilfælde.

Da endvidere -1 er ikkerest for 4, maa, i (6), u være lige, v ulige.

Betegner

(7) $u = A_n$, $v = B_n$, $n = 1, 2, 3, \ldots$

løsningerne af (6), har Lagrange vist, hvorledes alle disse løsninger bestemmes ved hjælp af konvergenterne i kædebrøken, der fremstiller $\sqrt{a}$.

Er A_1 og B_1 bestemt, findes de følgende løsninger ved hjælp af Lagranges rekursionsformler

(8) $A_{n+p} = A_n A_p + a B_n B_p$, $B_{n+p} = A_n B_p + A_p B_n$,

hvor, for alle m,

(9) $A_m^2 - a B_m^2 = (-1)^m$.

Antages i den sidste (8) $p = n$, faas $B_{2n} = 2 A_n B_n$, saaledes at B_{2n} altid er lige, A_{2n} følgelig ulige; da nu tegnene i (4) og (5) er sammenhørende, bliver ~~den sidste~~ kongruensen (3), ifølge den sidste (2), altsaa i dette tilfælde

(10) $A_{2n} - (-1)^n \equiv 0 \pmod{a}$.

Som anvendelse vil vi bevise, at enhver af de ubestemte ligninger

(11) $ax^2 \pm 2x = y^2$

kan løses i hele tal og bestemme disse løsninger.

Multipliceres (11) med a, faas

$$(ax \pm 1)^2 - ay^2 = 1,$$

og altsaa haves, ifølge (10) for det øverste fortegn

(12) $x = \dfrac{A_{4n} - 1}{a}$, $y = B_{4n}$,

medens det nederste fortegn giver

(12 bis) $x = \frac{A_{4n+2}+1}{a}$, $y = B_{4n+2}$.

Antages dernæst i (2) x lige, faas de til (4) svarende ligninger

(13) $x \pm 1 = 2u^2$, $x \mp 1 = av^2$,

hvor u og v er indbyrdes primiske, og hvor $y = uv$; heraf findes altsaa

(14) $u^2 - av^2 = \pm 2$,

hvor det positive tegn svarer til $a = 8n+7$, det negative til $a = 8n+3$.

Ligningen (14) kan altsaa altid løses i dette tilfælde, man faar nemlig

(15) $u^2 - av^2 = (-1)^{k+1} \cdot 2$.

Anvendes betegnelserne (7) ogsaa i dette tilfælde, altsaa

$$A_n^2 - a B_n^2 = 1,$$

gælder Lagranges rekursionsformler ogsaa i dette tilfælde, saaledes at B_{2n} stedse er lige; vort x i (13) er derfor stedse et A_{2n+1}, hvilket giver kongruensen

(16) $A_{2n+1} + (-1)^k \equiv 0 \pmod{a}$; $a = 4k+3$.

Som en anvendelse af de udviklede resultater vil vi vise, at ligningen

(17) $ax^2 + 2x = y^2$, naar $a = 8k+7$,

kan løses i hele tal og bestemme alle disse løsninger.

Omskrives (17) til

$$(ax+1)^2 - a y^2 = 1,$$

fraskrives dernæst ved (16)

(18) $x = \frac{A_{2n}-1}{a}$, $y = B_{2n}$, $a = 8k+7$.

Er $a = 8k+3$ kan derimod ligningen

$$ax^2 - 2x = y^2$$

løses i hele tal; man finder nemlig paa samme maade som før

(18 bis) $x = \frac{A_{2n+1}+1}{a}$, $y = B_{2n+1}$.

76. Antages $a = 2$, skal man bevise formlerne

$$A_{2n} = 2A_n^2 - (-1)^n = 4B_n^2 + (-1)^n,$$
$$B_{2n+1} = B_n^2 + B_{n+1}^2,$$
$$A_{2n+1} = A_{n+1}^2 - A_n^2 + (-1)^n = 2B_{n+1}^2 - 2B_n^2 - (-1)^n.$$

77. Bestem to paa hinanden følgende kvadrattal, hvis sum er et kvadrattal.

78. Bestem de trigonaltal, der tillige er kvadrattal.

79. Reducer ved en transformation ligningen $3x^2 - 2y^2 = 1$ til $u^2 - 6v^2 = 1$.

80. Bestem de oktagonaltal, der tillige er kvadrattal.

81. Bestem de pentagonaltal, som tillige er kvadrattal.

82. Bestem to trigonaltal, af hvilke det ene er det dobbelte af det andet.

83. Bestem de positive hele n og p, for hvilke henholdsvis

$$1 + 2 + 3 + \cdots + n = (n+1) + (n+2) + \cdots + (n+p)$$
$$1 + 2 + 3 + \cdots + n = p^2.$$

84. Løs ligningen $1 + x + x^2 = 3y^2$ i positive hele tal for x og y.

KAPITEL VII.

Kvadrattal og bikvadrattal.

§ 26. Pytagoræiske tal.

Ved *Pytagoræiske* tal forstaas systemer af tre hele tal, der angiver længderne af siderne i en retvinklet trekant, maalte i samme enhed; for at bestemme saadanne tal kommer det altsaa an paa at løse ligningen

(1) $$x^2 + y^2 = z^2$$

i positive hele tal.

Ved løsningen af denne opgave kan vi aabenbart indskrænke os til at betragte det tilfælde, hvor hvilkesomhelst to af tallene x, y og z er indbyrdes primiske; ti ethvert primtal, som gaar op i to af disse tal, maa ligeledes gaa op i det tredje, og denne primfaktors kvadrat kan derfor bortdivideres af (1).

Da en sum af to ulige kvadrattal er af formen $8n + 2$, kan en saadan sum aldrig være et kvadrattal; i de indbyrdes primiske løsninger af (1) maa z derfor altid være ulige, medens x og y er af modsat paritet.

Antages y lige, og skrives (1) paa formen

$$x^2 = (z^2 - y^2) = (z + y)(z - y), \tag{2}$$

maa de to ulige tal $z + y$ og $z - y$ være indbyrdes primiske; ti enhver fælles faktor for disse tal maa gaa op i tallenes sum og differens, altsaa i $2z$ og $2y$, og følgelig baade i z og y, hvilket er umuligt. Altsaa haves ifølge (2)

$$z + y = p^2, \quad z - y = q^2, \quad x = pq,$$

hvor p og q er indbyrdes primiske ulige tal, og derved findes løsningerne af (1):

$$z = \frac{p^2 + q^2}{2}, \quad y = \frac{p^2 - q^2}{2}, \quad x = pq. \tag{3}$$

Er y lige, og skrives (1) paa formen

$$y^2 = (z - x)(z + x), \tag{4}$$

faar faktorerne $z - x$ og $z + x$ største fælles faktor 2, og altsaa erholdes i dette tilfælde

$$z + x = 2p^2, \quad z - x = 2q^2, \quad y = 2pq,$$

hvor p og q er indbyrdes primiske og af modsat paritet; derved findes følgende løsninger af (1)

$$z = p^2 + q^2, \quad x = p^2 - q^2, \quad y = 2pq. \tag{5}$$

Den almindelige løsning af (1) findes hos *Euklid;* men *Pytagoras* og *Platon* skal have angivet hver sit specielle tilfælde, nemlig henholdsvis

Til ethvert A_{2n+1} svarer en ligning (13); betragtes denne ligning, faas

$$(u^2 + (-1)^k) - a(uv)^2 = 1;$$

løsningerne (u, v) til denne ligning danner derfor en følge

$$(u_1, v_1), (u_2, v_2), \ldots, (u_n, v_n), \ldots,$$

saaledes at

$$A_{2n+1} = u_n^2 + (-1)^k, \quad B_{2n+1} = u_n \cdot v_n. \tag{19}$$

Endvidere vil vi bevise sætningen:

Hvis ligningen

$$x^2 - ay^2 = b, \tag{20}$$

hvor b er et ulige tal, være o. ig. positivt eller negativt, kan løses i hele tal, kan en og kun en af ligningerne

$$x^2 - 4ay^2 = \pm b \tag{21}$$

opgaaes i hele tal.

Antages y lige, udleder (21) umiddelbart af (20); er y derimod ulige, maa x være lige. Multipliceres i dette tilfælde (20) med

$$A_1^2 - a B_1^2 = \pm 1,$$

faas

$$(A_1 x \pm a B_1 y)^2 - a(B_1 x \pm A_1 y)^2 = \pm b,$$

og her er $B_1 x \pm A_1 y$ et lige tal, fordi baade A_1 og x lige.

$$(2\alpha^2 + 2\alpha + 1)^2 = (2\alpha^2 + 2\alpha)^2 + (2\alpha + 1)^2$$
$$(\alpha^2 + 1)^2 = (\alpha^2 - 1)^2 + (2\alpha)^2.$$

Som en direkte anvendelse af de *Pytagoræiske* tal vil vi bevise sætningen:

I. *De positive hele, indbyrdes primiske løsninger af ligningen*

(6) $$x^2 + y^2 = 2z^2$$

bestemmes ved udtrykkene

(7) $z = \alpha^2 + \beta^2$, $x = \pm(\alpha^2 - \beta^2 + 2\alpha\beta)$, $y = \pm(\alpha^2 - \beta^2 - 2\alpha\beta)$,

hvor α *og* β *er indbyrdes primiske og af modsat paritet.*

Med de stillede krav ser man, at x, y og z alle maa være ulige tal; sættes

$$x = p + q, \quad y = p - q,$$

maa p og q være indbyrdes primiske og af modsat paritet, og man finder ved (6) ligningen

$$p^2 + q^2 = z^2,$$

hvorefter udtrykkene (7) umiddelbart dannes.

Ved bestemmelsen af x, y og z har vi altsaa fundet den almindelige form for tre kvadrattal, som danner en differensrække.

---

85. Ligningen $x^2 + 2y^2 = z^2$ skal løses i hele indbyrdes primiske tal.

86. Ligningen $x^2 + 2y^2 = 3z^2$ skal ved en transformation reduceres til den foranstaaende.

87. Vis, at den nødvendige og tilstrækkelige betingelse for, at ligningerne

$$x^2 - ay^2 = u^2, \quad x^2 + ay^2 = v^2$$

samtidig kan løses i hele tal, er, at

$$ay_1^2 = 4\alpha\beta(\alpha + \beta)(\alpha - \beta),$$

hvor y_1 er hel, medens α og β kan antages indbyrdes primiske og af modsat paritet[1]). Eks. $a = 6$[2]).

---

[1]) *Lucas*: Nouvelles Annales (2) Bd. 15, p. 466—470; 1876. (2) Bd. 17, p. 446—454; 1878.

[2]) Dette specielle tilfælde skyldes *Fermat*.

$$(2\alpha^2 + 2\alpha + 1)^2 = (2\alpha^2 + 2\alpha)^2 + (2\alpha + 1)^2$$
$$(\alpha^2 + 1)^2 = (\alpha^2 - 1)^2 + (2\alpha)^2.$$

Som en direkte anvendelse af de *Pytagoræiske* tal vil vi bevise sætningen:

I. *De positive hele, indbyrdes primiske løsninger af ligningen*

$$x^2 + y^2 = 2z^2 \tag{6}$$

bestemmes ved udtrykkene

$$z = \alpha^2 + \beta^2, \quad x = \pm(\alpha^2 - \beta^2 + 2\alpha\beta), \quad y = \pm(\alpha^2 - \beta^2 - 2\alpha\beta), \tag{7}$$

hvor α *og* β *er indbyrdes primiske og af modsat paritet.*

Med de stillede krav ser man, at x, y og z alle maa være ulige tal; sættes

$$x = p + q, \quad y = p - q,$$

maa p og q være indbyrdes primiske og af modsat paritet, og man finder ved (6) ligningen

$$p^2 + q^2 = z^2,$$

hvorefter udtrykkene (7) umiddelbart dannes.

Ved bestemmelsen af x, y og z har vi altsaa fundet den almindelige form for tre kvadrattal, som danner en differensrække.

---

85. Ligningen $x^2 + 2y^2 = z^2$ skal løses i hele indbyrdes primiske tal.

86. Ligningen $x^2 + 2y^2 = 3z^2$ skal ved en transformation reduceres til den foranstaaende.

87. Vis, at den nødvendige og tilstrækkelige betingelse for, at ligningerne

$$x^2 - ay^2 = u^2, \quad x^2 + ay^2 = v^2$$

samtidig kan løses i hele tal, er, at

$$ay_1^2 = 4\alpha\beta(\alpha + \beta)(\alpha - \beta),$$

hvor y_1 er hel, medens α og β kan antages indbyrdes primiske og af modsat paritet[1]). Eks. $a = 6$ [2]).

---

[1]) *Lucas*: Nouvelles Annales (2) Bd. 15, p. 466—470; 1876. (2) Bd. 17, p. 446—454; 1878.

[2]) Dette specielle tilfælde skyldes *Fermat*.

§ 27. Fermats og Eulers sætninger om bikvadrater.

De *Pytagoræiske* tal har spillet en vigtig rolle i flere af *Fermats* undersøgelser; som eksempel herpaa vil vi behandle følgende sætning, der skyldes *Fermat*[1]), og som er en af de faa sætninger, for hvilken den store talteoretikers bevis er os overleveret.

I. *Differensen mellem to forskellige bikvadrater, af hvilke intet er* 0, *kan aldrig være et kvadrattal.*

Vi behøver kun at undersøge ligningen

$$x^4 - y^4 = z^2, \quad x^4 = y^4 + z^2 \tag{1}$$

for positive hele indbyrdes primiske værdier af x, y og z. Ved denne undersøgelse vil vi antage, at x er det mindste positive hele tal, for hvilket (1) er mulig.

Man ser umiddelbart, at x altid maa være ulige; ti et ulige kvadrattal kan aldrig modulo 4 give resten — 1.

1 0. Antages y ulige, haves ifølge § 26, (5)

$$x^2 = \alpha^2 + \beta^2, \quad y^2 = \alpha^2 - \beta^2, \quad z = 2\alpha\beta, \tag{2}$$

hvor α og β er indbyrdes primiske og af modsat paritet. Da y^2 er af formen $4m + 1$, maa vi altsaa antage α ulige og β lige.

Af (2) faas imidlertid

$$\alpha^4 - \beta^4 = (xy)^2, \quad 0 < \alpha < x;$$

men dette er i strid med vor forudsætning om, at x^4 var det mindste bikvadrattal, som tilfredsstillede (1).

2 0. Antages y lige, haves derimod

$$x^2 = \alpha^2 + \beta^2, \quad z = \alpha^2 - \beta^2, \quad y^2 = 2\alpha\beta, \tag{3}$$

hvor α og β stedse er af modsat paritet og indbyrdes primiske.

Antages α ulige, β altsaa lige, faas af udtrykket for y^2

$$\alpha = p^2, \quad \beta = 2q^2, \quad y = 2pq,$$

---

[1]) Œuvres, Bd. I, p. 340—341.

hvor p er ulige, p og q indbyrdes primiske; men herefter findes af udtrykket for x^2

$$x = r^2 + s^2, \quad \alpha = r^2 - s^2, \quad \beta = 2rs = 2q^2,$$

hvor r og s paany er indbyrdes primiske og af modsat paritet. Af udtrykket for β faas derved

$$r = r_1^2, \quad s = s_1^2,$$

og altsaa erholdes

$$\alpha^2 = p^2 = r_1^4 - s_1^4, \quad 0 < r_1 \leqq \beta < x;$$

men det er umuligt, ifølge vor forudsætning om x.

Ganske paa samme maade behandles det tilfælde, hvor α er lige, β derimod ulige.

Af I faas følgende specielle tilfælde af *Fermats* berømte, hidtil ubeviste sætning [1]):

II. *En sum af to indbyrdes primiske bikvadrater kan aldrig være et bikvadrat. Ligningen*

$$x^4 + y^4 = z^4 \tag{4}$$

er uløselig i positive hele, indbyrdes primiske tal.

Til disse sætninger af *Fermat* har *Euler* [2]) føjet følgende:

III. *Ligningen*

$$x^4 + 4y^4 = z^2 \tag{5}$$

er uløselig i positive hele, indbyrdes primiske tal.

Da x og y begge maa være ulige, faas af (5)

$$x^2 = \alpha^2 - \beta^2, \quad 2y^2 = 2\alpha\beta, \quad \alpha = p^2, \ \beta = q^2,$$

hvor p og q er indbyrdes primiske; men derved kommer man til den, ifølge I, uløselige ligning

$$x^2 = p^4 - q^4.$$

IV. *Ligningen*

$$x^4 + y^4 = 2z^2 \tag{6}$$

er uløselig i positive hele, indbyrdes primiske tal.

---

[1]) *Ligningen* $x^n + y^n = z^n$ *er, for* $n > 2$, *uløselig i positive hele, indbyrdes primiske værdier af* x, y *og* z. Se f. eks. Œuvres, Bd. I, p. 291.

[2]) Commentarii Academiæ Petropolitanæ, Bd. 10 (1738), p. 130—139; 1747.

Man finder nemlig af (6) efter en simpel omformning

$$z^4 - (xy)^4 = \left(\frac{x^4 - y^4}{2}\right)^2,$$

hvilket ifølge I er umuligt.

V. *En sum af to indbyrdes primiske bikvadrater kan aldrig være et kvadrattal: Ligningen*

(7) $$x^4 + y^4 = z^2$$

kan ikke løses i positive hele indbyrdes primiske tal [1]).

Vi antager, at z er det mindste positive hele tal, for hvilken (7) er mulig, og vi lader f. eks. x være det ulige tal paa venstre side i (7); da haves

(8) $$x^2 = \alpha^2 - \beta^2, \quad y^2 = 2\alpha\beta, \quad z = \alpha^2 + \beta^2,$$

og her maa α være ulige, β lige; ti ellers kan x^2 ikke være et ulige kvadrattal. Af udtrykket for y^2 findes derfor

$$\alpha = p^2, \quad \beta = 2q^2, \quad y = 2pq,$$

hvor p er ulige og primisk med q; men derved erholdes af udtrykket for x^2

$$x^2 = p^4 - 4q^4,$$

og altsaa finder man

$$p^2 = r^2 + s^2, \quad x = r^2 - s^2, \quad q^2 = rs,$$

hvor r og s er indbyrdes primiske; derved erholdes af udtrykket for q^2

$$r = r_1^2, \quad s = s_1^2,$$

og altsaa haves

$$p^2 = r_1^4 + s_1^4, \quad p < \alpha < z;$$

men dette er i strid med vor forudsætning om, at z var det mindste positive hele tal, som tilfredsstillede en ligning af formen (7).

VI. *Ligningen*

(9) $$x^4 - y^4 = 2z^2$$

kan ikke løses i positive hele indbyrdes primiske tal for x, y og z.

---

[1]) Denne sætning skyldes dog *Fermat*. Œuvres, Bd. II, p. 431.

Da x og y begge maa være ulige, z derimod lige, findes

$$(10) \qquad x^2 + y^2 = 2\alpha^2, \quad x^2 - y^2 = 4\beta^2, \quad z = 2\alpha\beta;$$

af den anden af disse ligninger erholdes

$$x = p^2 + q^2, \quad y = p^2 - q^2, \quad \beta = pq,$$

og altsaa findes ved den første (10)

$$x^2 + y^2 = 2\alpha^2 = 2p^4 + 2q^4, \quad p^4 + q^4 = \alpha^2,$$

hvilket i følge V er umuligt.

Af IV og VI findes endvidere følgende sætning, der skyldes *Fermat* [1]), og som senere er genfunden af *Euler* [2]), men som hyppig tilskrives *Legendre* [3]):

VII. *Tallet* 1 *er det eneste trigonaltal, der kan være et bikvadrat.*

Var nemlig

$$(11) \qquad \frac{x(x+1)}{2} = y^4, \quad x(x+1) = 2y^4,$$

havdes, fordi x og $x + 1$ er indbyrdes primiske, enten

$$x = 2p^4, \quad x + 1 = q^4, \quad y = pq$$

eller

$$x = q^4, \quad x + 1 = 2p^4, \quad y = pq,$$

hvilket giver betingelserne

$$q^4 \pm 1^4 = 2p^4,$$

og dette er kun muligt, naar man læser det øverste fortegn og sætter $p = q = 1$, hvilket atter giver $x = y = 1$.

Skrives (11) paa formen

$$(12) \qquad (2x+1)^2 = 8y^4 + 1,$$

ser man, at denne sidste ligning ikke tilfredsstilles af andre positive hele tal end $x = 1$, $y = 1$.

---

[1]) Œuvres, Bd. II, p. 402.

[2]) Commentarii Academiæ Petropolitanæ, Bd. 10 (1738), p. 140—141 1747.

[3]) Théorie des nombres, Bd. II, p. 7. Zahlenteorie, Bd. II, p. 8.

Da x og y begge maa være ulige, z derimod lige, findes

$$x^2 + y^2 = 2\alpha^2, \quad x^2 - y^2 = 4\beta^2, \quad z = 2\alpha\beta; \tag{10}$$

af den anden af disse ligninger erholdes

$$x = p^2 + q^2, \quad y = p^2 - q^2, \quad \beta = pq,$$

og altsaa findes ved den første (10)

$$x^2 + y^2 = 2\alpha^2 = 2p^4 + 2q^4, \quad p^4 + q^4 = \alpha^2,$$

hvilket i følge V er umuligt.

Af IV og VI findes endvidere følgende sætning, der skyldes *Fermat* [1]), og som senere er genfunden af *Euler* [2]), men som hyppig tilskrives *Legendre* [3]):

VII. *Tallet* 1 *er det eneste trigonaltal, der kan være et bikvadrat.*

Var nemlig

$$\frac{x(x+1)}{2} = y^4, \quad x(x+1) = 2y^4, \tag{11}$$

havdes, fordi x og $x + 1$ er indbyrdes primiske, enten

$$x = 2p^4, \quad x + 1 = q^4, \quad y = pq$$

eller

$$x = q^4, \quad x + 1 = 2p^4, \quad y = pq,$$

hvilket giver betingelserne

$$q^4 \pm 1^4 = 2p^4,$$

og dette er kun muligt, naar man læser det øverste fortegn og sætter $p = q = 1$, hvilket atter giver $x = y = 1$.

Skrives (11) paa formen

$$(2x + 1)^2 = 8y^4 + 1, \tag{12}$$

ser man, at denne sidste ligning ikke tilfredsstilles af andre positive hele tal end $x = 1$, $y = 1$.

---

[1]) Œuvres, Bd. II, p. 402.

[2]) Commentarii Academiæ Petropolitanæ, Bd. 10 (1738), p. 140—141 1747.

[3]) Théorie des nombres, Bd. II, p. 7. Zahlenteorie, Bd. II, p. 8.

88. Bevis, at af de i opg. 76 betragtede tal A_n og B_n (svarende til $a = 2$) er $A_1 = 1$ det eneste A_n, der kan være et kvadrat og $B_2 = 2$ det eneste B_{2n}, der kan være det dobbelte af et kvadrat.

§ 28. Andre anvendelser af de Pytagoræiske tal.

Fermat[1]) har i et brev til *Frénicle* angivet følgende sætning:

I. *De eneste positive hele værdisæt af x, y og z, som tilfredsstiller ligningerne*

$$x = 2y^2 - 1, \quad x^2 = 2z^2 - 1 \tag{1}$$

er $x = y = z = 1$ *og* $x = 7$, $y = 2$, $z = 5$.

Man har længe forgæves søgt at bevise denne sætning; *Pepin*[2]) angav f. eks., at hvis ligningerne (1) skulde have andre løsninger end de af *Fermat* angivne, maatte disse skrives med mindst 3849 cifre! Omtrent samtidig lykkedes det *Genocchi*[3]) at finde følgende bevis:

Elimineres x af (1), findes

$$y^4 + (y^2 - 1)^2 = z^2; \tag{2}$$

antages y ulige, kan man ifølge § 26, (3) sætte

$$z = \frac{p^2 + q^2}{2}, \quad y^2 - 1 = \frac{p^2 - q^2}{2}, \quad y^2 = pq, \tag{3}$$

hvor p og q er ulige hele og indbyrdes primiske tal; udtrykket for y^2 giver da

$$p = m^2, \quad q = n^2,$$

hvoraf ved (3) af udtrykkene for y^2 og $y^2 - 1$:

$$m^2n^2 - 1 = \frac{m^4 - n^4}{2}, \quad (m^2 - n^2)^2 = 2(n^4 - 1),$$

hvoraf, idet $m^2 - n^2 = 2r$,

[1]) Œuvres Bd. II, p. 434. Baade *Fermats* brev og *Frénicles* svar synes nu tabte.

[2]) Atti della Accademia Pontificia dei Nuovi Lincei, Bd. 36, p. 23—33; 1884.

[3]) Nouvelles Annales (3), Bd. 2, p. 306—310; 1885.

Vis, at den ubestemte ligning $1 + x^2 + x^4 + x^6 = y^2$ ikke har andre positive hele løsninger end $x=1, y=2$.

$$n^4 - 1 = 2r^2,$$

og denne ligning er ifølge § 27, VI kun mulig for $n = 1$, $r = 0$, hvilket giver $x = y = z = 1$.

Antages y lige, faas af (2) ved anvendelse af § 26, (5)

$$z^2 = p^2 + q^2, \quad y^2 = 2pq, \quad y^2 - 1 = p^2 - q^2;$$

af udtrykket for $y^2 - 1$ ser man, at p maa være lige, q derimod ulige, medens p og q stedse kan antages indbyrdes primiske. Af udtrykket for y^2 findes dernæst

$$p = 2m^2, \quad q = n^2, \quad y^2 = 4m^2n^2, \quad y^2 - 1 = 4m^2n^2 - 1 = 4m^4 - n^4,$$

og altsaa erholdes

$$(2m^2 + n^2)^2 = 8m^4 + 1,$$

og denne ligning er ifølge § 27, (12) kun mulig for $m = n = 1$, hvilket giver $y = 2$, $x = 7$, $z = 5$.

Vi vil endnu her meddele følgende bevis af *Gerono*[1]) for sætningen:

II. *De eneste positive hele løsninger for x, y og z, som tilfredsstiller ligningerne*

(4) $$x = 4y^2 + 1, \quad x^2 = z^2 + (z + 1)^2,$$

er $x = 5$, $y = 1$, $z = 3$.

Antages z ulige, findes ved § 23, (5)

(5) $$x = \alpha^2 + \beta^2, \quad z = \alpha^2 - \beta^2, \quad z + 1 = 2\alpha\beta,$$

hvor de indbyrdes primiske tal α og β altsaa maa tilfredsstille betingelsen

(6) $$\beta^2 + 2\alpha\beta - \alpha^2 = 1,$$

hvoraf følger, at β er ulige og α lige; ti ellers maatte venstre side modulo 4 give resten -1.

Af den første ligning (4) faar man derpaa under anvendelse af (5) og (6)

$$2y^2 = \alpha(\alpha - \beta); \quad \alpha = 2p^2, \quad \alpha - \beta = q^2, \quad y = pq;$$

[1]) Nouvelles Annales (2) Bd. 17, p. 521—523; 1878.

ti tallene α, β og $\alpha - \beta$ er indbyrdes primiske, og α er et lige tal; indsættes disse udtryk for α og β i (6), findes

(7) $\qquad q^4 - 8p^2q^2 + 8p^4 + 1, \quad q^2 = 4p^2 \pm \sqrt{8p^4 + 1},$

og altsaa erholdes ved § 27, (12) $p = q = 1$, $y = 2$, $\alpha = 2$, $\beta = 1$, $x = 5$, $z = 3$.

Antages z lige, faas paa samme maade ved § 23, (5)

$$x = \alpha^2 + \beta^2, \quad z = 2\alpha\beta, \quad z + 1 = \alpha^2 - \beta^2,$$

hvoraf betingelsen

(8) $$\alpha^2 - 2\alpha\beta - \beta^2 = 1,$$

og heraf sluttes, at α maa være ulige, β derimod lige; endvidere findes

$$\beta(\beta + \alpha) = 2y^2; \quad \beta = 2p^2, \ \alpha = q^2, \ y = pq;$$

indføres disse udtryk for α og β i (8), faas atter (7), og altsaa findes paa denne maade de samme løsninger som før.

Disse løsninger er derfor de eneste mulige.

---

89. Vis, at blandt de i opg. 76 definerede tal A_n og B_n (altsaa svarende til $a = 2$) er $B_1 = 1$ og $B_3 = 5$ de eneste løsninger af ligningen $B_{2n+1} = 4y^2 + 1$, hvor y er et helt tal.

90. Vis, at med de samme betegnelser som i foranstaaende opgave er $A_1 = 1$ og $A_3 = 7$ de eneste mulige løsninger af ligningen $A_{2n+1} = 2y^2 - 1$, hvor y er helt tal.

91. Bestem de positive hele værdier af x og y, som tilfredsstiller ligningen

$$1 + x + x^2 + x^3 = y^2.$$

92. Er n og x hele tal, der begge er større end 1, og sættes

$$A_n(x) = 1 + x + x^2 + \cdots + x^{n-1} + x^n,$$

findes der, for alle ovennævnte x, kun to kvadrattal blandt tallene

$$A_2(x), \ A_3(x), \ A_4(x), \ A_5(x), \ A_7(x), \ A_9(x), \ A_{11}(x), \ \ldots$$

nemlig $A_3(7) = 20^2$ og $A_4(3) = 11^2$ [1]).

[1]) Se opg. 17.

KAPITEL VIII.

Fermats og Wilsons sætninger.

§ 29. Eulers generalisation af Fermats sætning.

Pierre de Fermat[1]) har i et d. 18. oktober 1640 dateret brev til *Frénicle* uden bevis meddelt følgende sætning:

I. *Er p et primtal, a et vilkaarligt helt tal, som blot ikke er deleligt med p, haves*

$$a^{p-1} \equiv 1 \pmod{p}. \tag{1}$$

Det først publicerede bevis for denne sætning skyldes *Euler*[2]); men det samme bevis er tidligere fundet af *Leibniz*[3]).

Det er indlysende, at sætningen I ogsaa kan formuleres paa følgende maade:

II. *Er p et primtal, a et vilkaarligt helt tal, haves*

$$a^{p} \equiv a \pmod{p}. \tag{2}$$

Antages nemlig a delelig med p, er (2) indlysende; er a ikke delelig med p, maa a være primisk med p, og altsaa kan man ifølge § 5, II bortdividere a i kongruensen (2).

For nu at bevise (2) ved induktion bemærker vi, at denne kongruens aabenbart er rigtig for $a = 1$. Antages dernæst (2) rigtig for tallet a, og anvendes kongruenserne § 12, (7)

$$\binom{p}{r} \equiv 0 \pmod{p}, \quad 1 \leqq r \leqq p-1, \tag{3}$$

faas ved anvendelse af binomialformlen

$$(a+1)^p \equiv a^p + 1 \equiv a + 1 \pmod{p},$$

saaledes at kongruensen (2) ogsaa gælder for det nærmest højere tal $a+1$, hvis den gælder for a.

Skrives I paa formen

$$a^{p-1} = 1 + hp,$$

[1]) Varia opera mathematica, p. 163; 1679. Œuvres, Bd. II, p. 209.
[2]) Commentarii Acad. Petropolitanæ, Bd. 8, p. 141—146; 1736 (1741).
[3]) Mathematische Schriften ved J. C. Gerhardt, Bd. VII, p. 180.

er h et helt tal; opløftes her til p^{te} potens, faas ved binomialformlen og under anvendelse af (3)

$$a^{p\,(p-1)} \equiv 1 \pmod{p^2}, \quad a^{p\,(p-1)} = 1 + h_1 p^2;$$

fortsættes paa denne maade, og er q et vilkaarligt positivt helt tal, findes almindelig

$$a^{p^{q-1}(p-1)} \equiv 1 \pmod{p^q},$$

hvoraf, idet m betegner et vilkaarligt positivt helt tal,

$$a^{mp^{q-1}(p-1)} \equiv 1 \pmod{p^q}. \tag{4}$$

Er dernæst

$$n = p_1^{a_1} p_2^{a_2} \cdot \cdots \cdot p_r^{a_r} \tag{5}$$

et vilkaarligt helt tal opløst i sine primfaktorer, og betegner p_s en vilkaarlig af disse primfaktorer, faas ifølge (4), idet a er primisk med n,

$$a^{\varphi(n)} - 1 \equiv 0 \pmod{p_s^{a_s}}. \tag{6}$$

Da nu alle modulerne i de r kongruenser af formen (6) er indbyrdes primiske, faas ifølge § 3, VIII den af *Euler* [1]) givne udvidelse af *Fermats* sætning:

III. *Betegner n et vilkaarligt helt tal, og er a primisk med n, haves*

$$a^{\varphi(n)} \equiv 1 \pmod{n}. \tag{7}$$

Fermats sætning tør ikke vendes om; man tør altsaa ikke af kongruensen (1) slutte, at p er et primtal.

Man har f. eks. [2])

$$2^{2700} \equiv 1 \pmod{2701}; \tag{8}$$

og her er

$$2701 = 37 \cdot 73 = 36 \cdot 75 + 1 \tag{9}$$

et sammensat tal. Af (1) findes

$$2^{36} \equiv 1 \pmod{37},$$

og endvidere er

---

[1]) Novi Commentarii Academiæ Petropolitanæ, Bd. 8, p. 102; 1760—61 (1763).

[2]) *Lucas:* Théorie des nombres, Bd. I, p. 422—423; Paris 1891.

Vis, at en sum af to indbyrdes primiske Kvadrattal ikke kan være delelig med noget primtal af formen 4n+3.

Vis, at intet x bestemt ved $x^2-(4n+3)y^2=1$ kan være af formen $2z^2+1$.

$$2^9 = 512 \equiv 1 \pmod{73}, \quad 2^{36} \equiv 1 \pmod{37 \cdot 73};$$

opløftes den sidste af disse kongruenser til 75de potens, faas netop (8).

Abel[1]) stillede følgende opgave:

Kan $a^{p-1} - 1$, *hvor* p *er et primtal*, a *et helt tal beliggende mellem* 1 *og* p, *være delelig med* p^2?

Jacobi[2]) besvarede straks dette spørgsmaal bekræftende, idet han meddelte, at *Busch* havde vist, at kongruensen

$$a^{p-1} - 1 \equiv 0 \pmod{p^2}, \tag{10}$$

under de *Abelske* forudsætninger er mulig i følgende tilfælde:

$$p = 11,\ a = 3,\ a = 9;\quad p = 29,\ a = 14;\quad p = 37,\ a = 18.$$

Lucas[3]) bemærker, at $p = 3$ og $p = 487$ er de eneste primtal mindre end 1000, for hvilke

$$10^{p-1} \equiv 1 \pmod{p^2}. \tag{11}$$

W. Fr. Meyer[4]) har givet almindelige undersøgelser over kongruensen (10), medens bl. a. *Mirimanoff*[5]) har undersøgt resten af det hele tal $(a^{p-1} - 1) : p$ modulo p.

---

93. Bevis formlerne

$$\frac{2^{2n}-1}{2n+1} = \sum_{s=0}^{s=n-1} \binom{2n}{2s+1} \frac{1}{2s+2} = \sum_{s=0}^{s=n-1} \binom{2n}{2s} \frac{1}{2s+1}.$$

94. Antages $a^p - 1 \equiv 0 \pmod{n}$, haves for r positiv hel $a^{pn^r} - 1 \equiv 0 \pmod{n^{r+1}}$.

§ 30. **Dirichlets bevis for Fermats sætning.**

Lejeune Dirichlet[6]) har givet et meget elegant bevis for *Fermats* sætning; vi vil her straks udvide dette bevis saaledes, at det giver den *Eulerske* generalisation.

---

[1]) Crelles Journal, Bd. 3, p. 212; 1828. Œuvres, Bd. I, p. 619.
[2]) Crelles Journal, Bd. 3, p. 301—302; 1828; Werke, Bd. VI, p. 238—239.
[3]) Théorie des nombres, Bd. I, p. 423; Paris 1891.
[4]) Archiv der Mathematik und Physik, (3) Bd. 2, p. 141—146; 1902.
[5]) Crelles Journal, Bd. 115, p. 295—300; 1895.
[6]) Crelles Journal, Bd. 3, p. 392; 1828. Werke, Bd. I, p. 103.

Lad n være et vilkaarligt helt tal, medens

(1) $$a_1,\ a_2,\ a_3,\ \ldots,\ a_\varphi$$

er de $\varphi(n)$ tal, der er mindre end eller lig med n og indbyrdes primiske med n, da vil de $\varphi(n)$ kongruenser af første grad

(2) $$ax \equiv a_r \pmod{n}, \quad r = 1,\ 2,\ 3,\ \ldots,\ \varphi(n),$$

hvor $a > 1$ ligeledes er primisk med n, for alle r have følgende egenskaber:

1 ^{0}. Kongruensen kan løses, og værdierne for x er indbyrdes primiske med n; altsaa eksisterer der et og kun et x tilfredsstillende (2), saaledes at

(3) $$1 \leqq x \leqq n - 1, \quad x \neq a_r.$$

2 ^{0}. Til to forskellige værdier af a_r svarer der, for det samme a, ligeledes to forskellige værdier af x tilfredsstillende (3); ti ellers fik man

$$a_r \equiv a_s \pmod{n}, \quad r \neq s,$$

hvilket er umuligt.

Det er derfor muligt at ordne de $\varphi(n)$ tal i (1) paa en saadan maade forskellig fra (1):

$$b_1,\ b_2,\ b_3,\ \ldots,\ b_\varphi,$$

at for

$$r = 1,\ 2,\ 3,\ \ldots,\ \varphi(n)$$

bestandig

(4) $$ab_r \equiv a_r \pmod{n}.$$

Multipliceres alle disse $\varphi(n)$ kongruenser af formen (4), faas

(5) $$a^{\varphi(n)}\, b_1 b_2 b_3 \cdots b_\varphi \equiv a_1 a_2 a_3 \cdots a_\varphi \pmod{n};$$

da nu i (5) de ligestore produkter

$$b_1 b_2 \cdots b_\varphi = a_1 a_2 \cdots a_\varphi$$

er indbyrdes primiske med n, erholdes

6) $$a^{\varphi(n)} \equiv 1 \pmod{n}$$

eller *Eulers* generalisation af *Fermats* sætning; ti det er indlysende, at (6) er rigtig for $a = 1$.

Angaaende yderligere beviser for *Fermats* sætning maa vi her indskrænke os til at henvise til *G. Wertheims* sidste bog [1]).

§ 31. Gauss's generalisation af Wilsons sætning.

Waring [2]) bemærker, at student *John Wilson* har meddelt ham, at $(p-1)! + 1$ altid vil være delelig med p, saafremt p er et primtal; men hverken *Wilson* eller *Waring* har kunnet bevise denne sætning.

Waring skriver, at »beviset synes saameget vanskeligere, fordi man ikke kan tænke sig nogen *betegnelse*, der formaar at udtrykke et primtal.«

Hertil bemærker *Gauss* [3]) ikke uden en vis, berettiget spydighed: »efter vor mening maa slige sandheder snarere øses af *begreber* end af betegnelser.«

Gauss [4]) har givet følgende generalisation af *Wilsons* sætning:

I. *Betegner n et vilkaarligt helt tal, og er*

$$a_1,\ a_2,\ a_3,\ \ldots,\ a_\varphi \tag{1}$$

de $\varphi(n)$ *positive hele tal, der højst er lig med n og indbyrdes primiske med n, haves stedse*

$$a_1 a_2 a_3 \cdots a_\varphi \equiv \pm 1 \pmod{n}. \tag{2}$$

De $\varphi(n)$ kongruenser

$$a_r x \equiv 1 \pmod{n}, \quad r = 1,\ 2,\ 3,\ \ldots,\ \varphi(n) \tag{3}$$

har aabenbart lignende egenskaber som kongruensen § 30, (2); det maa derfor være muligt at udtage visse par af tallene (1)

---

[1]) Anfangsgründe der Zahlenlehre, pp. 119—124, 232—233. Braunschweig 1902.

[2]) Meditationes algebraicæ, p. 218; London 1770.

[3]) Disquisitiones arithmeticæ, art. 76. Untersuchungen über höhere Arithmetik, p. 54; Berlin 1889. Werke, Bd, I, p. 61.

[4]) loc. cit. art. 78. Untersuchungen, p. 54—55. Werke, Bd. I, p. 61—62.

$$a_1 a_2 a_3 \cdots a_m$$
$$b_1 b_2 b_3 \cdots b_m,$$

saaledes at bestandig

$$a^s b_s \equiv 1 \pmod{n}, \quad s = 1, 2, 3, \ldots, m,$$

hvoraf ved multiplikation

(4) $$a_1 a_2 a_3 \cdots a_m \cdot b_1 b_2 b_3 \cdots b_m \equiv 1 \pmod{n}.$$

Tilbage har vi altsaa kun at betragte de tilfælde, hvor (3) giver $a_r = b_r$, altsaa hvor

(5) $$a_r^2 \equiv 1 \pmod{n};$$

af (5) faas imidlertid

(6) $$(n - a_r)^2 \equiv 1 \pmod{n},$$

og endvidere er

(7) $$a_r (n - a_r) \equiv -1 \pmod{n}.$$

Løsningerne af kongruensen (5), blandt tallene (1), forekommer derfor i lige antal, og disse løsninger kan ordnes parvis, saaledes at løsningerne i hvert par tilfredsstiller (7).

Multipliceres endelig (4) med alle kongruenserne af formen (7), faas *Gauss's* sætning; man ser, at fortegnet paa højre side i (2) retter sig efter antallet af rodpar i (5) indeholdte blandt tallene (1). *Gauss*[1]) har givet regler for bestemmelsen af dette fortegn; men det vil føre os for vidt her at gaa nærmere ind paa dette spørgsmaal.

Er $n = p$ et primtal, kan (5) kun være mulig, naar

$$a_r \equiv \pm 1 \pmod{p},$$

altsaa naar $a_r = 1$ eller $a_r = p - 1$; da man i dette tilfælde kun finder et rodpar i (5), erholdes *Wilsons* sætning:

II. *For ethvert primtal p gælder kongruensen*

(8) $$(p - 1)! + 1 \equiv 0 \pmod{p}.$$

Erstattes i ovenstaaende bevis n med primtallet p, skyldes det saaledes modificerede bevis *Euler*[2]).

---

[1]) Disquisitiones arithmeticæ art. 78. Untersuchungen, p. 54—55. Werke, Bd. I, p. 61—62.

[2]) Opuscula analytica, Bd. 1, p. 329—330; St. Petersborg 1783.

Af kongruensen (4) faas følgende anden form for *Wilsons* sætning:

III. *For ethvert primtal p gælder kongruensen*

$$(p-2)! - 1 \equiv 0 \pmod{p}. \tag{9}$$

For sammensatte tal haves sætningen:

IV. *Er $n > 4$ et sammensat tal, gælder kongruensen*

$$(n-1)! \equiv 0 \pmod{n}. \tag{10}$$

Haves $n = ab$, hvor $a \neq b$ og $a > 1$, $b > 1$, maa baade a og b findes som faktorer i $(n-1)!$, og (10) er indlysende. Er $n = p^2$, hvor p er et primtal, vil følgende multipla af p være mindre end $n - 1$:

$$p,\ 2p,\ 3p,\ \ldots,\ (p-1)p \tag{11}$$

og derfor findes som faktorer i $(n-1)!$. Antages $n \geqq 3$, indeholder (11) mindst to multipla af p, og altsaa gælder (10).

For $n = 4$, altsaa $p = 2$, faas $3! = 6$, altsaa ikke delelig med 4.

Da 6 modulo 4 er kongruent med 2, faas af II og IV den til II svarende omvendte sætning:

V. *Den nødvendige og tilstrækkelige betingelse for, at tallet p er et primtal, er, at*

$$(p-1)! + 1 \equiv 0 \pmod{p}.$$

Denne sætning er dog, paa grund af den uhyre voksen af $(p-1)!$ med p, uden nogen praktisk betydning.

---

95. Idet p er et primtal, og $0 \leqq q \leqq p - 1$, haves [1])

$$q!\,(p-q-1)! \equiv (-1)^{q+1} \pmod{p};$$

hvilken sætning kan man med *Lagrange* [2]) heraf udlede for $q = \frac{1}{2}(p-1)$?

---

[1]) Nouvelle correspondance mathématique, Bd. 5, pp. 156—160, 177—182; 1879.

[2]) Nouveaux Mémoires de l'Académie de Berlin, Bd. 2 (1771), p. 131; (1773).

96. Er $2n+1$ et primtal, haves

$$\frac{2^{2n}-1}{2n+1} \equiv 2^{n-1} \cdot 3 \cdot 5 \cdot 7 \cdot \cdots \cdot (2n-1)\, C_{n+1}^{n-1} \pmod{(2n+1)},$$

hvor C_{n+1}^{n-1} er den sædvanlige fakultetkoefficient.

§ 32. Lagranges bevis for Fermats og Wilsons sætninger.

Vi skal endnu vise, hvorledes *Lagrange* [1]) ved betragtning af fakultetet

$$(1) \quad x(x+1)\cdots(x+p-1) = C_p^0 x^p + C_p^1 x^{p-1} + \cdots + C_p^{p-1} x$$

under et har bevist baade *Fermats* og *Wilsons* sætninger.

Da p er et primtal, haves kongruenserne

$$(2) \quad \begin{cases} C_p^1 = \dfrac{p(p-1)}{2} \equiv 0 \pmod{p}; \quad \binom{p}{r} \equiv 0 \pmod{p}, \\ 1 \leqq r \leqq p-1; \end{cases}$$

under anvendelse af den i § 16 beviste formel (10)

$$(r-1)\, C_p^{r-1} = \binom{p}{r} C_p^0 + \binom{p-1}{r-1} C_p^1 + \cdots + \binom{p-r+2}{2} C_p^{r-2},$$

der er gyldig for $2 \leqq r \leqq p-1$, faas ved induktion de $p-2$ kongruenser

$$(3) \qquad C_p^r \equiv 0 \pmod{p}, \quad 1 \leqq r \leqq p-2.$$

Sættes dernæst i (1) $x = a$, hvor a er et hvilketsomhelst helt tal, erholdes umiddelbart ved anvendelse af (3)

$$(4) \quad a(a+1)\cdots(a+p-1) \equiv a^p + (p-1)!\, a \pmod{p};$$

ti man har $C_p^0 = 1$ og $C_p^{p-1} = (p-1)!$.

Er i (4) $a = 1$, bliver venstre side $p!$, og altsaa findes *Wilsons* sætning [2]):

---

[1]) Nouveaux Mémoires de l'Académie de Berlin, Bd. 2 (1771) p. 125—137; 1773.

[2]) Dette bevis for *Wilsons* sætning er det tidligst publicerede af alle. Sammenlign p. 96, note 2.

(5) $$(p-1)! + 1 \equiv 0 \pmod{p},$$

hvorefter (4) omskrives til

(6) $$a(a+1)\cdots(a+p-1) \equiv a^p - a \pmod{p}.$$

Da nu venstre side i (6) er produktet af p paa hinanden følgende hele tal, er dette produkt altid deleligt med p, og altsaa findes *Fermats* sætning:

(7) $$a^p - a \equiv 0 \pmod{p}.$$

---

97. Idet p er et primtal, og $p > 2r+1 \geqq 3$, haves

$$1^{2r+1} + 2^{2r+1} + \cdots (p-1)^{2r+1} \equiv 0 \pmod{p^2}.$$

98. Hvis $p > 3$ er et primtal, og $3 \leqq 2r+1 \leqq p-2$, haves

$$C_p^{2r+1} \equiv 0 \pmod{p^2}.$$

§ 33. **Fermats og Mersennes tal.**

For at meddele nogle af *Fermats* egne anvendelser af hans berømte sætning vil vi forudskikke følgende hjælpesætning:

I. *Er p et primtal, og betegner n den mindste positive hele eksponent, for hvilken*

(1) $$a^n \equiv 1 \pmod{p},$$

hvor a er et helt tal, som ikke er deleligt med p, saa er enhver anden eksponent m, for hvilken

(2) $$a^m \equiv 1 \pmod{p},$$

altid delelig med n.

Var nemlig m ikke delelig med n, fik man

$$m = nq + r, \quad 0 < r < n,$$

og altsaa havdes

$$a^m = (a^n)^q a^r \equiv a^r \equiv 1 \pmod{p},$$

hvilket er umuligt.

Da (2) i hvert fald er rigtig for $m = p - 1$, maa n altid gaa op i $p - 1$.

Som en første anvendelse af I vil vi betragte tal af formen

$$2^n - 1; \tag{3}$$

disse tal kan i hvert fald ikke være primtal, naar n er et sammensat tal. Haves nemlig $n = pq$, hvor $p \geqq q > 1$, er tallet i (3) deleligt baade med $2^p - 1$ og med $2^q - 1$; man finder f. eks.

$$2^n - 1 = (2^p)^q - 1 = (2^p - 1)(2^{n-p} + 2^{n-2p} + \cdots + 2^p + 1).$$

Om tallene af formen (3) har *Fermat* angivet følgende sætning, der først er bevist af *Euler*[1]):

II. *Er n et ulige primal, kan tallet $2^n - 1$ kun være deleligt med primtal af formen*

$$p = 2nq + 1. \tag{4}$$

Haves nemlig, idet n og p er primtal,

$$2^n - 1 \equiv 0 \pmod{p},$$

maa n ifølge I gaa op i $p - 1$, og da $p - 1$ er lige, maa p være af formen (4).

Man har hidtil vist, at de 9 tal af formen (3), svarende til eksponenterne

$$n = 2,\ 3,\ 5,\ 7,\ 13,\ 17,\ 19,\ 31,\ 61, \tag{5}$$

er primtal; de 8 første af disse tal kendtes allerede af *Euler*[2]), medens det sidste i den nyeste tid er behandlet af *Seelhoff*[3]),

---

[1]) Commentarii Academiæ Petropolitanæ, Bd. 6, p. 103—107; 1732—33 (1738). Novi Commentarii Academiæ Petropolitanæ, Bd. 1, p. 23; 1748—49 (1750). Commentationes arithmeticæ collectæ, Bd. I, pp. 1, 51.

[2]) Beviset for, at $2^{31} - 1$ er et primtal, har *Euler* givet i Histoire de l'Académie de Berlin 1772, p. 36; (1774).

[3]) Mathesis, Bd. 6, pp. 100—101, 178; 1886. Zeitschrift für Mathematik und Physik, Bd. 31, p. 174—178; 1886.

pastor *Perwuschin*[1]) og *Hudelot*[2]). Alle andre tal af denne form med eksponenter mindre end 61 er sammensatte tal[3]).

Som vi har set i § 13, svarer der til ethvert primtal af formen (3) et lige fuldkomment tal og omvendt.

Mersenne[4]) angiver, at der for $n \leqq 257$ kun eksisterer 11 primtal af formen (3), nemlig svarende til

$$n = 2,\ 3,\ 5,\ 7,\ 13,\ 17,\ 19,\ 31,\ 67,\ 127,\ 257; \tag{6}$$

denne angivelse er altsaa urigtig; ti primtallet 61 findes ikke i rækken (6).

F. N. Cole[5]) har paavist en anden fejl i *Mersennes* angivelse, idet primtallet $n = 67$ maa slettes; man finder nemlig

$$2^{67} - 1 = 193\,707\,721 \cdot 761\,838\,257\,287. \tag{7}$$

Oberst *Cunningham*[6]) har i 1908 vist, at $n = 71$ giver et sammensat tal[7]) af formen (3), idet

$$2^{71} - 1 = 228\,479 \cdot 10\,334\,355\,636\,337\,793. \tag{8}$$

Teoretiske undersøgelser over tallene af formen (3) skyldes

---

[1]) Jahrbuch über die Fortschritte der Mathematik, Bd. 19 (1887), p. 169.

[2]) Se *Lucas* i Mathesis, Bd. 7, p. 45—46; 1887.

[3]) Tallet $2^n - 1$ vides at være sammensat for følgende værdier af primtallet n: $n = 11,\ 23,\ 37$: *Fermat* i Varia opera mathematica, p. 164; Toulouse 1679. $n = 29,\ 37,\ 43,\ 73$: *Euler* i Commentarii Academiæ Petropolitanæ, Bd. 6, p. 105; 1732—33 (1738). $n = 41$: *Plana* i Memorie della Reale Accademia di Torino, Bd. 20, p. 130; 1863. $n = 43,\ 47,\ 53,\ 59$: *Landry* i Décompositons des nombres $2^n \pm 1$ en leurs facteurs premiers de $n = 1$ à $n = 64$; Paris 1869. $n = 37,\ 41,\ 43,\ 47,\ 53$: *Seelhoff* i Archiv der Mathematik und Physik (2) Bd. 2, p. 327—329; 1885. Bd. 5, p. 221—223; 1887. $n = 73,\ 79,\ 97,\ 113,\ 211,\ 223,\ 233$: *Le Lasseur*; se *Lucas* i American Journal of math., Bd. 1, p. 236. $n = 83,\ 131,\ 179,\ 191,\ 239,\ 251$: *Lucas* loc. cit.

[4]) Cogitata physico-mathematica, præfatio generalis, art. 19; Paris 1644.

[5]) Jahrbuch über die Fortschritte der Mathematik, Bd. 34, p. 216 (1903).

[6]) L'Intermédiaire des mathématiciens, Bd. 16, p. 252; 1909.

[7]) *Mersennes* ovenstaaende postulat er altsaa endnu usikkert for primtallene $n = 89,\ 101,\ 103,\ 107,\ 109,\ 127,\ 137,\ 139,\ 149,\ 157,\ 163,\ 167,\ 173,\ 181,\ 193,\ 197,\ 19$ 27, 229, 241, 257.

Lucas[1]), medens *Landry*[2]) for $1 \leqq n \leqq 64$ har givet tavler over divisorerne i tallene

$$2^n \pm 1.$$

Om tal af formen $2^n + 1$ bemærker vi, at disse tal i hvert fald ikke kan være primtal, med mindre eksponenten n er en potens af 2.

Havdes nemlig $n = p \cdot q$, hvor $q > 1$ er et ulige tal, er tallet

$$2^n + 1 = (2^p)^q + 1$$

deleligt med $2^p + 1 \geqq 3$. Om tal af formen $2^{2^n} + 1$ gælder sætningen:

III. *Tallet* $2^{2^n} + 1$ *kan kun være deleligt med primtallet* p, *naar dette er af formen*

(9) $$p = 2^{n+1}q + 1.$$

Haves nemlig

10) $$2^{2^n} \equiv -1 \pmod{p},$$

hvor p er et primtal, faas ved at kvadrere

$$2^{2^{n+1}} \equiv 1 \pmod{p};$$

men heraf følger, at 2^{n+1} er den mindste positive hele eksponent, for hvilken en kongruens af formen

$$2^a \equiv 1 \pmod{p}$$

kan bestaa; ti ellers maatte a være alikvot del af 2^{n+1}, hvilket ifølge (10) er umuligt.

Af I følger da umiddelbart, at primtallet p maa være af formen (9).

Da *Gauss*[3]) har vist, at de eneste regulære polygoner, der kan konstrueres ved passer og lineal, er saadanne, hvis sideantal er produkter af lutter forskellige primtal af formen

(11) $$E_n = 2^{2^n} + 1,$$

[1]) American Journal of math., Bd. 1, pp. 184—251, 289—321; 1878.

[2]) Décompositions des nombres $2^n \pm 1$; Paris 1869.

[3]) Disquisitiones arithmeticæ, art. 365—366. Untersuchungen über höhere Arithmetik, p. 446—448; Berlin 1889. Werke, Bd. I, p. 461—463.

vilde det være af stor interesse at have et simpelt middel til at afgøre, for hvilke n tallet E_n er et primtal, og at vide, om der eksisterer uendelig mange primtal af denne form.

Ganske vist har *Lucas* [1]), *Pepin* [2]), *Proth* [3]) og andre angivet betingelser, som skal opfyldes, for at E_n kan være et primtal; men de saaledes dannede regler er uden praktisk værdi.

De tal af formen (11), som svarer til følgende værdier af n:

(12) $$n = 5,\ 6,\ 12,\ 23,\ 36,$$

er i hvert fald sammensatte, nemlig henholdsvis delelige med

(13) 641, 274 177, 114 689, 167 772 161, 2 748 779 069 441.

E_5 er allerede undersøgt af *Euler* [4]), E_6 af *Landry* [5]), E_{12} og E_{23} af pastor *Perwuschin* [6]), E_{12} samtidig af *Lucas* [7]), og E_{36} af *Seelhoff* [8]).

Derimod er *Gauss's* [9]) bemærkning om, at *Fermat* [10]) skulde have hævdet, at han havde bevist, at tallene E_n altid, for alle n, var primtal, ikke helt rigtig; *Baltzer* [11]) og *Mansion* [12]) har gjort nærmere rede for dette forhold.

---

[1]) Comptes rendus, Bd. 85, p. 136—139; 1877.
[2]) Comptes rendus, Bd. 85, p. 329—331; 1877.
[3]) Comptes rendus, Bd. 87, p. 374; 1878.
[4]) Commentarii Academiæ Petropolitanæ, Bd. 6, p. 104; 1732—33 (1738). Commentationes arithmeticæ collectæ, Bd. I, p. 584; St. Petersborg 1849. Histoire de l'Académie de Berlin 1772, p. 36; (1774).
[5]) Nouvelle corresponpance mathématique, Bd. 6, p. 417: 1880.
[6]) Bulletin de l'Académie de Saint-Pétersbourg, Bd. 24, 25; 1878.
[7]) Atti de Torino, Bd. 13, p. 271—285; 1878.
[8]) Zeitschrift für Mathematik und Physik, Bd. 31, p. 174; 1886.
[9]) Disquisitiones arithmeticæ, art. 365. Untersuchungen über höhere Arithmetik, p. 446—447; Berlin 1889. Werke, Bd. I, p. 462.
[10]) Œuvres, Bd. II, pp. 208, 212—213.
[11]) Crelles Journal, Bd. 87, p. 172; 1879.
[12]) Nouvelle correspondance mathématique, Bd. 5, pp. 88—91, 122—125; 1879.

KAPITEL IX.

Kongruenser for primtalmodulus.

§ 34. Algebraiske kongruenser. Lagranges sætning.

Er

$$f(x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n$$

et vilkaarligt heltalligt polynomium af n^{te} grad, er altsaa samtlige koefficienter a_p hele tal, og er a_0 ikke delelig med det hele tal d, kaldes

$$f(x) \equiv 0 \pmod{d} \tag{1}$$

en algebraisk kongruens af n^{te} grad modulo d.

I (1) kommer kun hele værdier af x i betragtning; vi kan derfor straks udelade alle de led $a_p x^{n-p}$, som svarer til, at a_p er delelig med d.

Et helt tal α siges at være rod i kongruensen (1), naar det indsat istedetfor x tilfredsstiller denne kongruens.

Betegner x og m vilkaarlige hele tal, haves ifølge § 1, VI

$$f(x + md) \equiv f(x) \pmod{d};$$

hvis derfor α er rod i (1), vil $\alpha + md$ ligeledes være det. For at kende alle rødderne i (1) kan vi derfor indskrænke os til at undersøge saadanne rødder α, der tilfredsstiller betingelsen

$$0 \leqq \alpha \leqq d - 1; \tag{2}$$

disse rødder kaldes de inkongruente rødder i (1).

Ingen algebraisk kongruens modulo d kan derfor have mere end d inkongruente rødder.

Tilfredsstiller koefficienterne i $f(x)$ betingelserne

$$a_0 \equiv a_1 \equiv a_2 \equiv \cdots \equiv a_{n-1} \equiv a_n \equiv 0 \pmod{d}, \tag{3}$$

kaldes (1) en identisk kongruens modulo d; en saadan kongruens tilfredsstilles af alle mulige hele tal; men der eksisterer andre kongruenser med samme egenskab.

Betegner

(4) $$\omega_d(x) = x(x+1)\cdots(x+d-1)$$

fakultetet af ordenen d, er kongruensen

(5) $$\omega_d(x) \equiv 0 \pmod{d}$$

tilfredsstillet af alle mulige hele værdier af x.

Endvidere bemærker vi, at enhver hel rod i den algebraiske ligning $f(x) = 0$ tillige er rod i kongruensen (1), medens det omvendte i almindelighed ikke er tilfældet.

Divideres det heltallige polynomium $f(x)$ med $\omega_d(x)$, og sættes

(6) $$f(x) = \omega_d(x)\,\varphi(x) + \psi(x),$$

hvor $\psi(x)$ er den principale rest, bliver baade $\varphi(x)$ og $\psi(x)$ heltallige polynomier i x; ti i $\omega_d(x)$ har potensen x^d koefficienten 1.

Af (5) faas imidlertid ved (6) den for alle hele x gyldige kongruens

(7) $$f(x) \equiv \psi(x) \pmod{d}.$$

For at undersøge alle mulige algebraiske kongruenser modulo d behøver vi derfor kun at betragte saadanne, hvis grad aldrig overstiger $d-1$.

Er α en rod i kongruensen (1), giver identiteten

$$f(x) = (x-\alpha)f_1(x) + f(\alpha)$$

umiddelbart den for alle hele x gyldige kongruens

(8) $$f(x) \equiv (x-\alpha)f_1(x) \pmod{d}.$$

Efter disse almindelige bemærkninger vil vi udelukkende undersøge saadanne kongruenser, hvis modulus er et primtal p.

Ifølge *Fermats* sætning tilfredsstilles kongruensen af p^{te} grad

(9) $$x^p - x \equiv 0 \pmod{p},$$

ligesom den tilsvarende (5), af alle mulige hele værdier af x.

Disse kongruenser har mange egenskaber, som minder om algebraiske ligninger. Vi vil begynde med at bevise sætningen:

I. *Har kongruensen af n^{te} grad, hvor p er et primtal, og* $n \leqq p - 1$:

$$(10) \quad f(x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n \equiv 0 \pmod{p}$$

de n inkongruente rødder $\alpha_1, \alpha_2, \cdots, \alpha_n$, *haves for alle hele værdier af* x

$$(11) \quad f(x) \equiv a_0 (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n) \pmod{p}.$$

Af (8) findes en kongruens af formen

$$f(x) \equiv (x - \alpha_1) f_1(x) \pmod{p};$$

da nu p er et primtal, maa kongruensen af graden $n - 1$

$$f_1(x) \equiv 0 \pmod{p}$$

have rødderne $\alpha_2, \alpha_3, \cdots, \alpha_n$, og altsaa findes

$$f_1(x) \equiv (x - \alpha_2) f_2(x) \pmod{p},$$

hvoraf

$$f(x) \equiv (x - \alpha_1)(x - \alpha_2) f_2(x) \pmod{p}.$$

Fortsættes paa denne maade, findes tilsidst kongruensen (11).

Af (11) udledes atter følgende sætning, som skyldes *Lagrange* [1]:

II. *Er p et primtal, og $n \leqq p - 1$, maa enhver algebraisk kongruens af n^{te} grad modulo p, som har $n + 1$ inkongruente rødder, være en identisk kongruens modulo p.*

Er kongruensen den i (10) betragtede, og haves endvidere roden α_{n+1}, faas ifølge (11)

$$a_0 (\alpha_{n+1} - \alpha_1)(\alpha_{n+1} - \alpha_2) \cdots (\alpha_{n+1} - \alpha_n) \equiv 0 \pmod{p},$$

hvoraf man slutter, at p maa gaa op i a_0; ti alle de andre, fra 0 forskellige, faktorer paa venstre side er numerisk mindre end p, og derfor primiske med p. Vi behøver altsaa kun at undersøge kongruensen af graden $n - 1$

$$a_1 x^{n-1} + \cdots a_{n-1} x + a_n \equiv 0 \pmod{p};$$

fortsættes paa denne maade, ser man, at a_1 maa være delelig med p, o. s. v.

[1]) Mémoires de l'Académie de Berlin 1768, p. 192.

Af II faas atter sætningen:

III. *En ikke identisk algebraisk kongruens af n^{te} grad modulo p kan højst have n inkongruente rødder.*

Som et supplement til denne sætning bemærker vi, at det er let at angive algebraiske kongruenser, som overhovedet ikke har løsninger; dette er f. eks. tilfældet med

$$x^2 \equiv 3 \pmod 5.$$

Om disse forhold haves endvidere sætningen:

IV. *Den nødvendige og tilstrækkelige betingelse for, at den algebraiske kongruens af n^{te} grad*

$$f(x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n \equiv 0 \pmod p$$

har netop n inkongruente rødder, er, at den heltallige principale divisonsrest $\varphi(x)$ bestemt ved

$$a_0^{p-n+1}(x^p - x) = f(x)\, g(x) + \varphi(x) \tag{12}$$

giver en identisk kongruens

$$\varphi(x) \equiv 0 \pmod p. \tag{13}$$

Har nemlig den givne kongruens netop n inkongruente rødder, maa ifølge (12) det samme være tilfældet med (13), og denne kongruens maa altsaa være identisk, fordi den højst er af graden $n - 1$.

Er omvendt kongruensen (13) identisk, maa ifølge (12) kongruensen af p^{te} grad

$$f(x)\, g(x) \equiv 0 \pmod p \tag{14}$$

have p inkongruente rødder; da endvidere p er et primtal, er (14) ensbetydende med de to kongruenser af henholdsvis n^{te} og $(p - n)^{te}$ grad

$$f(x) \equiv 0 \pmod p, \quad g(x) \equiv 0 \pmod p,$$

og disse kongruenser maa derfor ifølge III have netop henholdsvis n og $p - n$ inkongruente rødder.

I beviset for IV kunde vi istedetfor (12) have benyttet identiteten

(15) $$a_0^{p-n+1}\,\omega_p(x) = f(x)\,g_1(x) + \varphi_1(x),$$

hvor $\varphi_1(x)$ er den principale rest.

Man ser, at betingelsen (13) er opfyldt, hvis $f(x)$ gaar op i $x^p - x$ eller i $\omega_p(x)$.

---

99. Hvilket middel har man til at afgøre, om to algebraiske kongruenser for samme modulus d har fælles rødder, og hvorledes bestemmes disse eventuelle fælles rødder?

100. Har kongruensen af n^{te} grad

$$x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n \equiv 0 \pmod{p},$$

hvor p er et primtal, og $n \leqq p - 1$, de n inkongruente rødder $\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_n$, og sætter man

$$s_r = \alpha_1^r + \alpha_2^r + \cdots \alpha_n^r,$$

haves for $1 \leqq r \leqq n$ kongruenserne

$$s_r + a_1 s_{r-1} + \cdots + a_{r-1}\,s_1 + r a_r \equiv 0 \pmod{p}.$$

101. Hvad ved man, med definitionerne § 34, (12) og (15), om kongruenserne

$$g(x) \equiv 0 \pmod{p}, \quad g_1(x) \equiv 0 \pmod{p}?$$

§ 35. **Fermats kongruens.**

Analogien mellem algebraiske kongruenser for en primtalmodulus p og algebraiske ligninger træder endnu stærkere frem ved en sammenligning mellem *Fermats* kongruens

(1) $$x^{p-1} - 1 \equiv 0 \pmod{p}$$

og den binome ligning.

Vi vil nærmere anskueliggøre denne analogi gennem følgende sætninger:

I. *Er n divisor i $p - 1$, har den binome kongruens af n^{te} grad*

$$x^n - 1 \equiv 0 \pmod{p} \tag{2}$$

netop n inkongruente rødder.

Sættes $p - 1 = nq$, gaar $x^n - 1$ op i $(x^n)^q - 1 = x^{p-1} - 1$, og I er en umiddelbar følge af § 34, IV.

II. *Er q og r begge divisorer i* $p - 1$, *bestemmes de for de binome kongruenser*

$$x^q - 1 \equiv 0 \pmod{p}, \quad x^r - 1 \equiv 0 \pmod{p} \tag{3}$$

fælles rødder ved kongruensen

$$x^f - 1 \equiv 0 \pmod{p}, \tag{4}$$

hvor f er største fælles faktor for q og r.

For $q = r$ er sætningen indlysende; antages dernæst f. eks. $q > r$, og sættes $q = rq_1 + r_1$, hvor $0 \leqq r_1 \leqq r - 1$, og er a en fælles rod for kongruenserne (3), haves

$$a^q = a^{q_1 r} \cdot a^{r_1} \equiv a^{r_1} \equiv 1 \pmod{p};$$

alle de fælles rødder for kongruenserne (2) maa derfor være rødder i kongruensen

$$x^{r_1} \equiv 1 \pmod{p},$$

og man ser, at den af polynomierne $x^q - 1$ og $x^r - 1$ dannede *Euklidiske* algoritme [1]) umiddelbart fører til maalet.

Paa samme maade bevises sætningen:

III. *Er n et vilkaarligt positivt helt tal, og betegner f største fæiles faktor for n og* $p - 1$, *har kongruensen*

$$x^n - 1 \equiv 0 \pmod{p}$$

netop f inkongruente rødder.

Betegner a et vilkaarligt af tallene 1, 2, 3, ..., $p - 1$, og er n den mindste positive hele eksponent, for hvilken

$$a^n \equiv 1 \pmod{p},$$

har vi i § 33, I bevist, at n er divisor i $p - 1$; under disse forudsætninger siger vi, at roden a hører til eksponenten n, og at a er primitiv rod i kongruensen

[1]) Se f. eks. min *Elementer af den nyere algebra*, p. 33; 1911.

(5) $$x^n \equiv 1 \pmod{p}, \quad p - 1 \equiv 0 \pmod{n}.$$

Med disse definitioner haves sætningerne:

IV. *Er a en primitiv rod i kongruensen* (5), *og er m indbyrdes primisk med n, er* a^m *ligeledes primitiv rod i* (5).

Havdes nemlig for $0 < q < n$

$$(a^m)^q = a^{mq} \equiv 1 \pmod{p},$$

maatte n ifølge § 33, I gaa op i mq; men det er umuligt, fordi n er primisk med m, og $q < n$.

V. *Hvis kongruensen* (5) *har en primitiv rod a, bliver alle rødderne i denne kongruens*

(6) $$1, \ a, \ a^2, \ a^3, \ \ldots, \ a^{n-1}.$$

Det ses nemlig umiddelbart, at alle potenserne (6) er rødder i kongruensen (5); det kommer altsaa kun an paa at vise, at alle tallene (6) to og to er inkongruente modulo p.

Havdes imidlertid for $r > s$

$$a^r \equiv a^s \pmod{p}, \quad a^{r-s} \equiv 1 \pmod{p},$$

kom man i strid med forudsætningen om, at a var en primitiv rod i (5); ti $r - s < n$.

Da ialt $\varphi(n)$ af eksponenterne i (6) er primiske med n, ser vi ved anvendelse af IV, at kongruensen (5) maa have netop $\varphi(n)$ primitive rødder, hvis den overhovedet har nogen saadan rod.

Er $\psi(n)$ antallet af primitive rødder i (5), haves derfor enten $\psi(n) = \varphi(n)$ eller $\psi(n) = 0$.

Er dernæst $d_1, d_2, d_3, \ldots, d_r$ samtlige divisorer i $p - 1$, maa et hvilketsomhelst af tallene 1, 2, 3, $\ldots$, $p - 1$, der jo alle er rødder i *Fermats* kongruens (1), høre til en af disse divisorer som eksponent, og altsaa haves

$$\psi(d_1) + \psi(d_2) + \cdots + \psi(d_r) = p - 1;$$

sammenholdes denne ligning med den i § 11, III angivne formel

$$\varphi(d_1) + \varphi(d_2) + \cdots + \varphi(d_r) = p - 1,$$

102. Man finder $a^2+a+1 \equiv 0 \pmod p$ altsaa $(a+1)^3+1 = a^3+3a+3a+2$ $\equiv 3(a^2+a+1) \equiv 0 \pmod p$, hvoraf $(a+1)^3+1 \equiv 0 \pmod p$; $a+1$ kan derfor ikke høre til exponenten 3. Det er indlysende, at $a+1$ ikke kan høre til exponenten 1; antages dernæst $(a+1)^2 \equiv 1 \pmod p$, fæas $a(a+2) \equiv 0 \pmod p$, hvilket er umuligt, altsaa kan $a+1$ ikke høre til exponenten 6.

og erindres det, at man for ethvert s har enten $\psi(d_s) = \varphi(d_s)$ eller $\psi(d_s) = 0$, er aabenbart kun den første af disse ligheder mulig, og altsaa haves sætningen:

VI. *Den binome kongruens* (5), *hvor n altsaa er divisor i* $p-1$, *har netop* $\varphi(n)$ *primitive rødder.*

Antages specielt $n = p-1$, faas

VII. *Antallet af primitive rødder i Fermats kongruens er* $\varphi(p-1)$.

Disse sætninger skyldes *Gauss* [1]; VI kendtes af *Euler* [2]; men hans bevis for den er ufuldstændigt.

---

102. Hører a for primtalmodulus p til eksponenten 3, maa $a+1$ for samme modulus p høre til eksponenten 6 [3].

103. Er a_1 og a_2 inkongruente rødder i den binome kongruens

$$x^n \equiv 1 \pmod p,$$

hvor p er et primtal, n en alikvot del af $p-1$, kan $a_1 a_2 - 1$ aldrig være delelig med p.

§ 36. **Gauss's teori om tals indeks.**

Af § 35, V faas for $n = p-1$ specielt

I. *Er g en primitiv rod i Fermats kongruens*

$$x^{p-1} - 1 \equiv 0 \pmod p, \tag{1}$$

hvor p altsaa er et primtal, bliver alle rødderne i denne kongruens

$$1, g, g^2, g^3, \ldots, g^{p-2}. \tag{2}$$

Er derfor a et hvilketsomhelst af tallene

$$1, 2, 3, \ldots, p-1, \tag{4}$$

eksisterer der saaledes et tal α, som tilfredsstiller betingelserne

---

[1] Disquisitiones arithmeticæ, art. 53—54. Untersuchungen über höhere Arithmetik, p. 35—36; Berlin 1889. Werke, Bd. I, p. 43—44.

[2] Novi Commentarii Academiæ Petropolitanæ, Bd. 18, p. 85—135; 1773 (1774). Se navnlig p. 98.

[3] *Laisant* i Mémoires de Bordeaux (2) Bd. 2, p. 400—402; 1876.

(5) $$0 \leqq \alpha \leqq p - 2,$$

og for hvilket

(6) $$a \equiv g^{\alpha} \pmod{p};$$

denne eksponent α kaldes *indeks til a med basis g*, og man sætter

(7) $$\alpha = \operatorname{ind}_g a;$$

hvor ingen misforstaaelse kan finde sted, udelades g dog sædvanlig i denne betegnelse.

De saaledes definerede indices har mange egenskaber fælles med logaritmer; dog maa det vel erindres, at vi her for et givet primtal p ikke kan have flere indekssystemer, end der er primitive rødder i (1), altsaa ialt $\varphi(p-1)$, medens vi kan vælge et hvilketsomhelst fra 1 forskelligt tal til basis i et logaritmesystem og i dette finde logaritmerne af alle mulige andre tal.

Den ovennævnte analogi mellem indices og logaritmer træder tydelig frem gennem følgende sætninger:

II. *Indeks af et produkt er modulo $p-1$ kongruent med summen af faktorernes indices.*

Sæ tes

$$\alpha = \operatorname{ind} a, \quad \beta = \operatorname{ind} b,$$

haves

$$a \equiv g^{\alpha} \pmod{p}, \quad b \equiv g^{\beta} \pmod{p}, \quad ab \equiv g^{\alpha+\beta} \pmod{p},$$

og altsaa erholdes

8) $$\operatorname{ind}(ab) \equiv \operatorname{ind} a + \operatorname{ind} b \pmod{(p-1)}.$$

Af II faas umiddelbart:

III. *Indeks af en potens er modulo $p-1$ kongruent med rodens indeks multipliceret med potenseksponenten.*

I indeksteorien erstattes brøken $c = a : b$ med kongruensen

(9) $$bc \equiv a \pmod{p}.$$

Ved anvendelse af II findes dernæst:

IV. *Er intet af tallene a eller b deleligt med p, faas af* (9)

(10) $$\operatorname{ind} c \equiv \operatorname{ind} a - \operatorname{ind} b \pmod{(p-1)}.$$

Haves indekstavler for de forskellige primtal og en af de tilsvarende primitive rødder, kan man derved løse alle kongruenser af formen (9).

Af den i § 5 beviste sætning III følger umiddelbart, at enhver kongruens af første grad kan erstattes med flere andre, hvis moduler alle er primtal. Enhver kongruens af første grad, som overhovedet har løsninger, kan derfor løses ved indekstavler.

Om indices af samme tal svarende til forskellige primitive rødder som basis gælder sætningen:

V. *Er g_1 og g_2 to inkongruente primitive rødder i Fermats kongruens svarende til primtallet p, og er a et vilkaarligt helt tal, haves:*

$$\text{(11)} \qquad \operatorname{ind}_{g_1} a \equiv \operatorname{ind}_{g_2} a \cdot \operatorname{ind}_{g_1} g_2 \pmod{(p-1)}.$$

Sættes nemlig

$$\alpha_1 = \operatorname{ind}_{g_1} a, \quad \alpha_2 = \operatorname{ind}_{g_2} a, \quad \omega = \operatorname{ind}_{g_1} g_2,$$

haves

$$a \equiv g_1^{\alpha_1} \pmod{p}, \quad a \equiv g_2^{\alpha_2} \pmod{p}, \quad g_2 \equiv g_1^{\omega} \pmod{p},$$

og altsaa erholdes

$$a \equiv g_1^{\omega\alpha_2} \equiv g_1^{\alpha_1} \pmod{p},$$

hvoraf

$$\alpha_1 \equiv \omega\alpha_2 \pmod{(p-1)},$$

eller kongruensen (11).

Skønt indeksteorien allerede forekommer hos *Euler*[1]), er den dog først kommen til sin fulde ret gennem *Gauss's*[2]) undersøgelser. *C. G. J. Jacobi*[3]) har offentliggjort indekstavler svarende til alle primtal under 1000.

---

[1]) Commentationes arithmeticæ collectæ, Bd. I, p. 516—537; St. Petersborg 1849.

[2]) Disquisitiones arithmeticæ, art. 57—72. Untersuchungen über höhere Arithmetik, p. 38—50; Berlin 1889. Werke, Bd. I, p. 46—62.

[3]) Canon arithmeticus, sive tabulæ, quibus exhibentur pro singulis numeris primis vel primorum potestatibus infra 1000 numeri ad datos indices et indices ad datos numeros pertinentes; Berlin 1839.

§ 37. Perioder hørende til et tal.

Er p et primtal, n divisor i $p-1$, og hører tallet a til eksponenten n, er alle potenserne

$$1,\ a,\ a^2,\ \ldots,\ a^{p-2}, \tag{1}$$

sikkert rødder i kongruensen

$$x^n \equiv 1 \pmod{p};$$

men da (2) kun har n modulo p inkongruente rødder, kan de $p-1$ tal i (1) ikke alle være indbyrdes inkongruente modulo p.

Antages $nn_1 = p-1$, maa tallene i (1) dele sig i n_1 grupper med n tal i hver, nemlig

$$\begin{aligned}
&1,\ a,\ a^2,\ \ldots,\ a^{n-1}\\
&a^n,\ a^{n+1},\ a^{n+2},\ \ldots,\ a^{2n-1}\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
&a^{p-1-n},\ a^{p-n},\ a^{p-n+1},\ \ldots\ldots,\ a^{p-2},
\end{aligned}$$

saaledes at tallene i den enkelte gruppe er alle rødderne i (2), medens ethvert tal i en vilkaarlig gruppe er kongruent med et og kun et tal i en vilkaarlig anden gruppe.

De tal, der tilhører en og samme gruppe, siges at danne en til tallet a svarende periode; om disse perioder gælder følgende sætninger, der skyldes *Gauss*[1]):

I. *Er P produktet af alle tallene i en til tallet n hørende periode, haves*

$$P \equiv (-1)^{n-1} \pmod{p}. \tag{3}$$

Man finder nemlig

$$P \equiv a^{1+2+3+\ldots+n-1} \equiv a^{\frac{n(n-1)}{2}} \pmod{p}. \tag{4}$$

Er dernæst n ulige, bliver $n-1$ lige, og eksponenten til a i sidste led af (4) er et multiplum af n; i dette tilfælde haves altsaa

$$P \equiv 1 \pmod{p}. \tag{5}$$

[1]) Disquisitiones arithmeticæ, art. 75, 79. Werke, Bd. I, pp. 60, 62. Untersuchungen über höhere Arithmetik, pp. 53, 55; Berlin 1889.

Antages n derimod lige, haves ifølge (2)

$$\left(a^{\frac{n}{2}}+1\right)\left(a^{\frac{n}{2}}-1\right) \equiv 0 \pmod{p},$$

og da p er en primitiv rod i (2), findes

$$a^{\frac{n}{2}} \equiv -1 \pmod{p},$$

hvoraf ifølge (4), idet $n-1$ er ulige,

$$P \equiv (-1)^{n-1} \equiv -1 \pmod{p}, \tag{6}$$

og af (5) og (6) følger I umiddelbart.

II. *Er S summen af alle tallene i en til tallet n hørende periode, haves*

$$S \equiv 0 \pmod{p}. \tag{7}$$

Man finder her

$$S \equiv 1 + a + a^2 + \cdots + a^{n-1} \pmod{p},$$

hvoraf ved multiplikation med $a-1$

$$(a-1)\,S \equiv a^n - 1 \equiv 0 \pmod{p},$$

og da primtallet p ikke kan gaa op i $a-1 < p$, faas netop (7).

§ 38. **Primitive rødder i Fermats kongruens.**

Vi tænker os stedse, at p er et primtal, vi opløser $p-1$ i primfaktorer som

$$p-1 = a_1^{\alpha_1}\, a_2^{\alpha_2} \cdots a_r^{\alpha_r}, \tag{1}$$

og vi skal derefter gaa over til at undersøge, hvorledes vi af de primitive rødder i hver enkelt af de r kongruenser modulo p

$$x^{a_1^{\alpha_1}} \equiv 1, \quad x^{a_2^{\alpha_2}} \equiv 1, \ \ldots, \ x^{a_r^{\alpha_r}} \equiv 1 \tag{2}$$

kan danne primitive rødder i *Fermats* kongruens

$$x^{p-1} - 1 \equiv 0 \pmod{p}. \tag{3}$$

Om dette spørgsmaal gælder sætningen:

I. *Betegner*

(4) $$q_1,\ q_2,\ \ldots,\ q_r$$

en vilkaarlig primitiv rod i hver sin af kongruenserne (2), *er produktet*

(5) $$q_1 \cdot q_2 \cdot q_3 \cdots q_r$$

en primitiv rod i (3), *og de* $\varphi(p-1)$ *mulige produkter af denne form fremstiller samtlige primitive rødder i* (3).

At produktet (4) tilfredsstiller kongruensen (3), er indlysende. Var nu dette produkt ikke nogen primitiv rod i (3), maa det høre til en eller anden eksponent, der er divisor i $p-1$, og som er mindre end $p-1$; denne eksponent maa derfor ligeledes være divisor i $(p-1):a_s$, hvor a_s er en af primfaktorerne i (1). Da man nu stedse har

$$\frac{p-1}{a_s} \equiv 0 \pmod{a_m^{\alpha_m}}, \quad m \neq s,$$

findes altsaa

$$(q_1 q_2 \cdots q_r)^{\frac{p-1}{a_s}} \equiv q_s^{\frac{p-1}{a_s}} \equiv 1 \pmod{p};$$

men det er umuligt; ti q_s hører til eksponenten $a_s^{\alpha_s}$, og $(p-1):a_s$ er kun delelig med $a_s^{\alpha_s-1}$.

Produktet (4) er derfor en primitiv rod i *Fermats* kongruens.

Da tallene $q_1, q_2, q_3, \ldots, q_r$ kan have henholdsvis

$$a_1^{\alpha_1-1}(a_1-1),\quad a_2^{\alpha_2-1}(a_2-1),\ \ldots,\ a_r^{\alpha_r-1}(a_r-1)$$

modulo p inkongruente værdier, faar produktet (4) ialt

$$a_1^{\alpha_1-1}(a_1-1)\,a_2^{\alpha_2-1}(a_2-1)\cdots a_r^{\alpha_r-1}(a_r-1) = \varphi(p-1)$$

værdier, og det kommer altsaa an paa at vise, at ikke to af disse værdier kan være indbyrdes kongruente modulo p.

Betegner d_s et tal mindre end og primisk med $a_s^{\alpha_s}$, kan man bestemme et positivt helt tal β_s, saaledes at man samtidig har

(6) $$\beta_s \equiv d_s \pmod{a_s^{\alpha_s}},\quad \beta_s \equiv 0 \pmod{(p-1):a_s^{\alpha_s}};$$

da nemlig $a_s^{\alpha_s}$ og $(p-1):a_s^{\alpha_s}$ er indbyrdes primiske, kan kongruensen

$$a_s^{\alpha_s}x + d_s \equiv 0 \pmod{(p-1):a_s^{\alpha_s}}$$

løses i hele værdier for x, og (6) er tilfredsstillet for

$$\beta_s = d_s + x a_s^{\alpha_s}. \tag{7}$$

Betegner dernæst d'_s et fra d_s forskelligt af tallene mindre end og primisk med $a_s^{\alpha_s}$, og sættes

$$\beta'_s \equiv d'_s \pmod{a_s^{\alpha_s}}, \quad \beta'_s \equiv 0 \pmod{(p-1):a_s^{\alpha_s}},$$

haves aabenbart

$$\beta_s - \beta'_s \equiv 0 \pmod{a_m^{\alpha_m}}, \quad m \neq s, \tag{8}$$

medens $\beta_s - \beta'_s$, ifølge (7), ikke kan være delelig med a_s.

Er dernæst g en primitiv rod i *Fermats* kongruens (3), hører g^{β_s} til eksponenten $a_s^{\alpha_s}$; ti for det første haves ifølge (6)

$$(g^{\beta_s})^{a_s^{\alpha_s}} \equiv 1 \pmod{p};$$

er endvidere m det mindste positive hele tal, for hvilket

$$(g^{\beta_s})^m = g^{\beta_s m} \equiv 1 \pmod{p},$$

maa $p-1$, da g er en primitiv rod i (3), gaa og i $\beta_s m$, hvilket ifølge den første kongruens (6) kun er muligt, naar $a_s^{\alpha_s}$ gaar op i m.

Potensen

$$g^{\beta_1+\beta_2+\cdots+\beta_r} \tag{9}$$

maa derfor ifølge I være en primitiv rod i (3). Det kommer derfor endnu kun an paa at bevise, at ikke to af potenserne (9) er indbyrdes kongruente modulo p.

Antages, med ovenstaaende definitioner af tallene β'_s,

$$g^{\beta_1+\beta_2+\cdots+\beta_r} \equiv g^{\beta'_1+\beta'_2+\cdots+\beta'_r} \pmod{p},$$

haves, idet (9) er en primitiv rod i (3),

$$\beta_1+\beta_2+\cdots+\beta_r \equiv \beta'_1+\beta'_2+\cdots+\beta'_r \pmod{(p-1)},$$

hvoraf ifølge (8)

$$\beta_s - \beta'_s \equiv 0 \pmod{a_s^{\alpha_s}},$$

hvilket, som vi ovenfor bemærkede, er umuligt.

Vi skal dernæst gaa over til at undersøge summen S og produktet P af samtlige primitive rødder i *Fermats* kongruens (3). Betegner

$$S_1,\ S_2,\ S_3,\ \ldots.,\ S_r$$

summen af de primitive rødder i hver enkelt af kongruenserne (2), faas ifølge I

$$S = S_1 S_2 S_3 \cdot \ldots \cdot S_r. \tag{10}$$

Antages i den første af kongruenserne (2) $\alpha_1 = 1$, findes ifølge § 37, II

$$S_1 \equiv -1 \pmod{p}; \tag{11}$$

ti alle rødderne i denne kongruens, med undtagelse af 1, er da primitive.

Haves derimod $\alpha_1 > 1$, og erindres det, at alle tallene mindre end $a_1^{\alpha_1}$ og delelige med a_1 er

$$a_1,\ 2a_1,\ 3a_1,\ \ldots.,\ a_1^{\alpha_1} - a_1,$$

findes i dette tilfælde modulo p

$$S_1 \equiv (1 + q_1 + q_1^2 + \cdots + q_1^{a_1^{\alpha_1 - 1}}) - (1 + q_1^{a_1} + q_1^{2a_1} + \cdots + q_1^{a_1^{\alpha_1 - a_1}}),$$

hvoraf

$$(q_1^{a_1} - 1)\, S_1 \equiv \left(\frac{q_1^{a_1} - 1}{q_1 - 1} - 1\right)(q_1^{a_1^{\alpha_1}} - 1) \equiv 0 \pmod{p},$$

og da q_1 hører til eksponenten $a_1^{\alpha_1} > a_1$, findes herved

$$S_1 \equiv 0 \pmod{p}. \tag{12}$$

Paa samme maade behandles de øvrige summer $S_2, S_3, \ldots. S_r$. Af kongruenserne (11) og (12) og de dermed analoge, faas derfor $S \equiv 0$, naar $p - 1$ er deleligt med nogen primtalspotens (hvis eksponent er større end 1).

Er $p - 1$ produktet af lutter forskellige primtal, faas kun kongruenser af formen (11), og altsaa erholdes $S \equiv \pm 1$, eftersom antallet af primfaktorer i $p - 1$ er lige eller ulige.

Sammenholdes dette resultat med den i § 16, eks. 4 givne definition, faas sætningen:

II. *Er S summen af de primitive rødder i Fermats kongruens* (3), *og betegner* $\mu(p-1)$ *den Möbius'ske faktor, haves*

$$S \equiv \mu(p-1) \pmod{p}. \tag{13}$$

For at undersøge produktet af de primitive rødder i (3), hvor p antages større end 3, betegner vi ved

$$d_1,\ d_2,\ d_3,\ \ldots.,\ d_\varphi \tag{14}$$

de $\varphi(p-1)$ tal, der er mindre end og primiske med $p-1$; er g en primitiv rod i (3), kan alle de primitive rødder i samme kongruens fremstilles ved potenserne

$$g^{d_1},\ g^{d_2},\ \ldots.,\ g^{d_\varphi},$$

og altsaa erholdes

$$P = g^{d_1+d_2+\ldots.+d_\varphi}. \tag{15}$$

Da tallene (14) er de samme som

$$p-1-d_1,\ \ p-1-d_2,\ \ \ldots.,\ p-1-d_\varphi,$$

blot tagne i en anden orden, faas

$$2(d_1+d_2+\cdots.+d_\varphi) = (p-1)\varphi(p-1);$$

da $\varphi(p-1)$, med vor forudsætning om p, er et lige tal, haves

$$d_1+d_2+\cdots.+d_\varphi = k(p-1),$$

hvor k er positiv hel, og altsaa erholdes ved (15) sætningen:

III. *For produktet P af de primitive rødder i Fermats kongruens* (3), *hvor* $p > 3$, *haves*

$$P \equiv 1 \pmod{p}. \tag{16}$$

Disse sætninger skyldes *Gauss*[1]).

Det er indlysende, at (16) ikke gælder for primtallet 3; ti i dette tilfælde haves kun den eneste primitive rod 2.

---

[1]) Disquisitiones arithmeticæ, art. 55, 80, 81. Untersuchungen über höhere Arithmetik, pp. 36—38, 55—57; Berlin 1889. Werke, Bd I, pp. 44—46, 62—64.

§ 39. Den almindelige binome kongruens.

Vi skal her endnu kort omtale kongruensen

$$x^m \equiv a \pmod{p}, \quad 1 < m < p-1, \tag{1}$$

hvor m er positiv hel, p et ulige primtal, som ikke gaar op i det hele tal a; om denne kongruens gælder sætningen:

I. *Den nødvendige og tilstrækkelige betingelse for, at* (1) *har løsninger, er, at a tilfredsstiller kongruensen*

$$a^{\frac{p-1}{f}} \equiv 1 \pmod{p}, \tag{2}$$

hvor f er største fælles faktor for m og p — 1; i dette tilfælde har (1) *f rødder.*

Opløftes (1) til potensen $(p-1):f$, og bemærkes det, at f gaar op i m, medens x ikke kan være delelig med p, ses det straks, at (2) er en nødvendig betingelse; ti man finder

$$x^{\frac{m}{f}(p-1)} \equiv a^{\frac{p-1}{f}} \equiv 1 \pmod{p}.$$

Sættes $m = m_1 f$, $p - 1 = m_2 f$, og bemærkes det, at m_1 og m_2 er indbyrdes primiske, er kongruensen

$$m_1 \alpha - 1 \equiv 0 \pmod{m_2} \tag{3}$$

opløselig med hensyn til α, og det samme gælder derfor

$$m\alpha - f \equiv 0 \pmod{(p-1)}. \tag{4}$$

Opløftes dernæst (1) til potensen α, faas ifølge (4)

$$x^f \equiv a^\alpha \pmod{p}, \tag{5}$$

og denne kongruens maa følgelig have alle rødderne i (1). For omvendt at vise, at alle rødderne i (5) tillige findes i (1), opløfter vi (5) til potensen m_1; derved erholdes ved (3) og (4)

$$x^m - a \equiv a\,(a^{m_1\alpha-1} - 1) \equiv a\left(a^{\frac{m\alpha-f}{f}} - 1\right) \equiv 0 \pmod{p};$$

ti eksponenten $(m\alpha - f):f$ er ifølge (4) et multiplum af den i (2) forekommende eksponent $(p-1):f$.

For endvidere at bestemme antallet af rødderne i (1) eller (5), gaar vi ud fra identiteten

$$x^p - x = x\left((x^f)^{\frac{p-1}{f}} - (a^\alpha)^{\frac{p-1}{f}}\right) + x\left((a^\alpha)^{\frac{p-1}{f}} - 1\right);$$

her er første led paa højre side deleligt med $x^f - a^\alpha$, og altsaa findes

$$x^p - x = (x^f - a^\alpha)\,\varphi(x) + x\left((a^\alpha)^{\frac{p-1}{f}} - 1\right),$$

hvor den principale divisionsrest giver en modulo p identisk kongruens.

Ifølge § 35, IV har (1) under forudsætningen (2) derfor netop f rødder.

---

104. Undersøg kongruensen $x^m + 1 \equiv 0 \pmod p$. Eks. 1. $p = 13$, $m = 4$. Eks. 2. $p = 13$, $m = 9$.

KAPITEL X.

Kvadratiske rester.

§ 40. Eulers kriterium. Legendres symbol.

Hvis kongruensen, hvor a er primisk med p,

$$x^2 \equiv a \pmod p \tag{1}$$

kan løses, kaldes a en kvadratisk rest eller blot en rest modulo p; har (1) derimod ingen løsning, kaldes a en kvadratisk ikkerest eller blot en ikkerest modulo p.

Her vil vi kun betragte kvadratiske rester og ikkerester hørende til et ulige primtal p. Kongruensen (1) er da et specielt tilfælde af den i § 39 betragtede, og man faar ved § 39, I umiddelbart følgende sætning, der sædvanlig kaldes *Eulers*[1]) kriterium:

[1]) Opuscula analytica, Bd. I, pp. 242, 268; St. Petersborg 1783.

I. *Den nødvendige og tilstrækkelige betingelse for, at tallet a er rest for det ulige primtal p, er, at*

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}. \tag{2}$$

Euler har dog ikke givet noget eksakt bevis for denne sætning.

Da endvidere

$$a^{p-1} - 1 = \left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right) \equiv 0 \pmod{p},$$

faas ved I den tilsvarende sætning:

II. *Er tallet a ikkerest svarende til det ulige primtal p, haves*

$$a^{\frac{p-1}{2}} \equiv -1 \pmod{p}. \tag{3}$$

Ifølge § 35, I har kongruensen (2) nøjagtig $\frac{1}{2}(p-1)$ inkongruente rødder, halvdelen af de $p-1$ tal

$$1, 2, 3, \ldots, p-1 \tag{4}$$

maa derfor være rester, de øvrige ikkerester modulo p.

Er endvidere n et vilkaarligt helt tal, haves

$$(np \pm b)^2 \equiv b^2 \pmod{p}; \tag{5}$$

ethvert kvadrattal, som ikke er deleligt med p, maa derfor modulo p være kongruent med et af kvadrattallene

$$1^2, 2^2, 3^2, \ldots, \left(\frac{p-1}{2}\right)^2; \tag{6}$$

af (5) faas endvidere sætningen:

III. *Er a en kvadratisk rest modulo p, har kongruensen* (1) *to rødder, hvis sum er p.*

For værdierne paa højre side i kongruenserne (2) og (3) har *Legendre*[1]) foreslaaet betegnelsen

$$\left(\frac{a}{p}\right),$$

der nu sædvanlig kaldes *Legendres* symbol; altsaa haves stedse

[1]) Théorie des nombres, Bd. I, p. 197. Zahlentheorie, Bd. I, p. 198.

Euler har bevist sit Kriterium: Opuscula analytica I, 263.

(7) $$\left(\frac{a}{p}\right) = \pm 1,$$

idet a ikke er delelig med p, og kongruenserne (2) og (3) kan bringes paa den fælles form

(8) $$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p},$$

hvorefter *Eulers* kriterium antager formen:

IV. *Tallet a er rest eller ikkerest modulo p, eftersom*

$$\left(\frac{a}{p}\right) = 1 \quad \textit{eller} \quad \left(\frac{a}{p}\right) = -1.$$

Antages $a \equiv b \pmod{p}$, faas ifølge definitionen af *Legendres* symbol

(9) $$\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right),$$

medens § 5, (4) i forbindelse med (8) umiddelbart giver

(10) $$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right),$$

hvoraf sætningen:

V. *Produktet af to rester eller to ikkerester er altid en rest, medens produktet af en rest og en ikkerest altid er en ikkerest.*

Af I faas umiddelbart følgende af *Fermat*[1]) angivne sætning, som første gang er bevist af *Euler*[2]):

VI. *Tallet -1 er rest for alle primtal af formen $4n+1$, men ikkerest for alle primtal af formen $4n+3$.*

Ved kombination af V og VI erholdes endelig:

VII. *For primtallene af formen $4n+1$ er a og $4n+1-a$ begge samtidig enten rester eller ikkerester.*

---

[1]) Varia opera mathematica, p. 168. Toulouse 1679.

[2]) Novi Commentarii Academiæ Petropolitanæ, Bd. 5, p. 3–58; 1754–55 (1760). Opuscula analytica, Bd. I, pp. 74, 135; St. Petersborg 1783.

105. Betegner $r_1, r_2, \ldots, r_n$ resterne, $i_1, i_2, \ldots, i_n$ ikkeresterne for et primtal $p = 2n + 1$, haves

$$r_1 \cdot r_2 \cdot r_3 \cdots r_n \equiv (-1)^{n+1} \pmod{p},$$
$$i_1 \cdot i_2 \cdot i_3 \cdots i_n \equiv (-1)^n \pmod{p}.$$

106. Er, med betegnelserne i opg. 105, det positive hele tal q ikke deleligt med n, haves

$$r_1^q + r_2^q + \cdots + r_n^q \equiv i_1^q + i_2^q + \cdots + i_n^q \equiv 0 \pmod{p}.$$

107. Er q positiv hel, findes derimod modulo p

$$r_1^{nq} + r_2^{nq} + \cdots + r_n^{nq} \equiv n, \quad i_1^{nq} + i_2^{nq} + \cdots + i_n^{nq} \equiv n + 1.$$

108. For primtallene p af formen $4n + 1$ haves

$$r_1 + r_2 + \cdots + r_{2n} = i_1 + i_2 + \cdots + i_{2n} = \frac{p(p-1)}{4}.$$

§ 41. Gauss's lemma.

Ved anvendelse af *Eulers* kriterium har *Gauss*[1]) givet en anden nødvendig og tilstrækkelig betingelse for, at det positive hele tal a, som ikke er deleligt med det ulige primtal p, er kvadratisk rest modulo p.

Det er aabenbart, at samtlige tal

$$(1) \qquad a,\ 2a,\ 3a,\ \ldots,\ \frac{p-1}{2}a$$

er indbyrdes primiske med p, og at ikke to af disse tal kan være kongruente modulo p; de modulo p numerisk mindste rester af tallene (1) maa derfor alle findes blandt tallene

$$\pm 1,\ \pm 2,\ \pm 3,\ \ldots,\ \pm\frac{p-1}{2}.$$

Betegner

$$(2) \qquad \beta_1,\ \beta_2,\ \beta_3,\ \ldots,\ \beta_r$$
$$(3) \qquad -\alpha_1,\ -\alpha_2,\ -\alpha_3,\ \ldots,\ -\alpha_s \Big\} \quad r + s = \frac{p-1}{2}$$

[1]) Commentationes Gottingenses, Bd. 16; 1808. Untersuchungen über höhere Arithmetik, p. 498; Berlin 1889. Werke, Bd. II, p. 51.

Hvis a er kvadratisk rest for k, er a ligeledes rest for en vilkaarlig potens af k, der fuldtöbig antages ulige.
Hvis a er kvadratisk rest for k, haves en ligning af formen
(1) $a = \alpha_1^2 - k\beta_1$,
hvor α_1 og β_1 er hele tal. Af (1) faas dernæst umiddelbart
(2) $a = (\alpha_1 + k\gamma_1)^2 - k(\beta_1 + 2\alpha_1\gamma_1 + k\gamma_1^2)$;
dernæst bestemmes γ_1 saaledes at
$$\beta_1 + 2\alpha_1\gamma_1 \equiv k\beta_2,$$
hvilket er muligt, fordi k og $2\alpha_1$ er indbyrdes primiske.
Derefter antages (2) formen
$$a = \alpha_2^2 - k\beta_2,$$
hvor α_2 og β_2 paany er hele tal; den fuldstændige
Induktion er indlysende.
Sætningen gælder ikke umiddelbart i denne form
for alle lige værdier af k.
Alle ulige tal er rester for 2, medens resterne for 4
og 8 er henholdsvis af formerne $4n+1$ og $8n+1$.
Antallet af rödder i kongruensen
(1) $x^2 \equiv a \pmod{k}$,
der tænkes opløselig, afhænger af antallet af primfaktorer
i k.
Er k ulige, og indeholder dette tal n primfaktorer,
$$k = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n},$$
har kongruensen (1) netop 2^n rödder.
Da a er rest modulo k, kan (1) ogsaa skrives paa
formen
$$x^2 \equiv \alpha^2 \pmod{k}$$
eller
$$(x+\alpha)(x-\alpha) \equiv 0 \pmod{k},$$
og k maa derfor kunne skrives som et produkt

af k_0 indføres primiske faktorer, $k = k_1 k_2$, saaledes at

(2) $x \pm \alpha \equiv 0 \pmod{k_1}$ $x \mp \alpha \equiv 0 \pmod{k_2}$.

Skal k_1 indeholde r primfaktorer, kan k_1 dannes paa $\binom{n}{r}$ forskjellige maader. Spaltningen $k = k_1 k_2$ kan derfor foretages paa

$$\frac{1}{2}\left(1 + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n-1} + 1\right) = 2^{n-1}$$

forskjellige maader, hvorefter (2) i hvert enkelt tilfælde giver to kongruenser, eftersom den ene eller den anden først tages, saaledes at antallet af rødderne bliver netop 2^n.

Er k et lige tal af formen $4m+2$, altsaa

$$k = 2 \cdot p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n},$$

bliver antallet af rødder atter 2^n. Haves derimod k af formen $8m+4$, altsaa

$$k = 4 \cdot p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n},$$

bliver antallet af rødder 2^{n+1}, fordi en vilkaarlig af faktorerne i (2) kan tænkes delelig med 4.

Er endelig k et multiplum af 8, altsaa

$$k = 2^r \cdot p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}, \quad r \geq 3,$$

bliver antallet 2^{n+2}, fordi en vilkaarlig af faktorerne i (2) kan tænkes delelig med 2^{r-1} eller med 2^r.

henholdsvis de positive og de negative numerisk mindste rester modulo p, kan ingen af de følgende kongruenser modulo p

$$\alpha_n \equiv \alpha_{n_1}, \quad \beta_n \equiv \beta_{n_1}, \quad \beta_n + \alpha_{n_1} \equiv 0$$

bestaa; ti det maatte medføre, at enten differensen eller summen af to af tallene i (1) var delelig med p, hvilket er umuligt.

Samlingen

$$\beta_1, \beta_2, \ldots, \beta_r; \quad \alpha_1, \alpha_2, \ldots, \alpha_s$$

maa altsaa være tallene

$$1, 2, 3, \ldots, \frac{p-1}{2}$$

tagne i en eller anden orden og hver medregnet en og kun en gang.

Man finder derfor

$$a^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \equiv (-1)^s \left(\frac{p-1}{2}\right)! \pmod{p},$$

hvoraf

$$a^{\frac{p-1}{2}} \equiv (-1)^s \pmod{p}, \tag{4}$$

og altsaa erholdes *Gauss's* lemma:

I. *Tallet a er kvadratisk rest modulo p, eftersom talrækken* (1) *giver et lige eller et ulige antal negative numerisk mindste rester modulo p.*

Anvendes *Legendres* symbol, faas af (4)

$$\left(\frac{a}{p}\right) = (-1)^s. \tag{5}$$

Vil man f. eks. anvende *Gauss's* lemma for $a = 2$, kommer det altsaa an paa at undersøge tallene

$$2, 4, 6, \ldots, p-1; \tag{6}$$

i dette øjemed bestemmer vi det positive hele tal k, saaledes at

$$p - 1 - 2k < \frac{p}{2} < p + 1 - 2k,$$

hvilket sker paa entydig maade; ti sættes $p = 2n + 1$, erholdes

(7) $$n - \tfrac{1}{2} < 2k < n + \tfrac{3}{2}, \quad n \leqq 2k \leqq n + 1.$$

Af tallene (6) giver følgende

$$p + 1 - 2k, \quad p + 3 - 2k, \quad \ldots, \quad p - 1,$$

og ikke andre, negative numerisk mindste rester modulo p, og altsaa haves ifølge (5)

(8) $$\left(\frac{2}{p}\right) = (-1)^k.$$

Da nu ethvert ulige tal kan skrives paa en af følgende fire former $8m \pm 1$ eller $8m \pm 3$, og da man ved (7) finder

(9) $$\begin{cases} p = 8m \pm 1, & n = 4m \quad \text{eller } n = 4m - 1, \; k = 2m \\ p = 8m \pm 3, & n = 4m + 1 \text{ eller } n = 4m - 2, \; k = 2m \pm 1, \end{cases}$$

faas følgende sætning, der er angiven af *Fermat*[1]), men først bevist af *Lagrange*[2]):

II. *Tallet 2 er rest for alle primtal af formen* $8m \pm 1$, *men ikkerest for alle primtal af formen* $8m \pm 3$.

Ligningen (8) kan bringes paa en overskueligere form, idet man af (9), for $p = 8m \pm 1$, $p = 8m \pm 3$, udleder

$$\frac{p^2 - 1}{8} = 8m^2 \pm 2m, \quad k = 2m,$$

$$\frac{p^2 - 1}{8} = 8m^2 \pm 6m + 1, \quad k = 2m \pm 1,$$

og altsaa erholdes sætningen:

III. *Er p et hvilketsomhelst ulige primtal, haves*

(10) $$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

---

[1]) Varia opera mathematica, p. 168; Toulouse 1679.

[2]) Nouveaux Mémoires de l'Académie de Berlin 1775. pp. 349, 351.

Af ligningerne

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}, \quad \left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)$$

findes ved anvendelse af (10)

$$\left(\frac{-2}{p}\right) = (-1)^{\frac{(p-2)^2-1}{8}}, \tag{11}$$

hvoraf sætningen, der ligeledes er angiven af *Fermat*, men først bevist af *Lagrange*:

IV. *Tallet* -2 *er rest for alle primtal af formen* $8m+1$ *eller* $8m+3$, *men ikkerest for alle primtal af formen* $8m-1$ *eller* $8m-3$.

---

109. Hvis a og b er indbyrdes primiske, er tal af formen a^2+2b^2 ikke delelige med noget primtal af formen $8n+5$ eller $8n+7$.

§ 42. **Reciprocitetssætningen for kvadratiske rester.**

Vi betragter nu de to ulige forskellige primtal p og q, hvor $q>p$; de modulo p numerisk mindste rester af tallene

$$q,\ 2q,\ 3q,\ \ldots,\ \frac{p-1}{2}q \tag{1}$$

betegnes ved

$$\left\{\begin{matrix}\beta_1,\ \beta_2,\ \ldots,\ \beta_\varkappa \\ -\alpha_1,\ -\alpha_2,\ \ldots\ -\alpha_\lambda\end{matrix}\right\}, \quad \varkappa+\lambda=\frac{p-1}{2}, \tag{2}$$

medens de tilsvarende rester modulo q af tallene

$$p,\ 2p,\ 3p,\ \ldots,\ \frac{q-1}{2}p \tag{3}$$

betegnes ved

$$\left\{\begin{matrix}\delta_1,\ \delta_2,\ \delta_3,\ \ldots,\ \delta_\mu \\ -\gamma_1,\ -\gamma_2,\ -\gamma_3,\ \ldots,\ -\gamma_\nu\end{matrix}\right\}, \quad \mu+\nu=\frac{q-1}{2}; \tag{4}$$

med disse betegnelser findes ifølge *Gauss's* lemma

(5) $$\left(\frac{q}{p}\right) = (-1)^{\lambda}; \quad \left(\frac{p}{q}\right) = (-1)^{\nu}, \quad \left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\lambda+\nu}.$$

Om resterne (2) og (4) gælder sætningen:

I. *Samtlige tal* α *findes blandt tallene* δ, *medens samtlige tal* β *findes blandt tallene* γ; *er endvidere* c *antallet af de rester* $-\gamma$, *for hvilke* $\gamma > \frac{1}{2}p$, *haves*

(6) $$\nu - \varkappa = c, \quad \lambda + \nu = \varkappa + \lambda + c = \frac{p-1}{2} + c,$$

og c *er da og kun da ulige, naar* q *er af formen* $4k+1$ *og* p *samtidig af formen* $4h-1$.

Sættes $hq = kp \pm x$, hvor x er en numerisk mindste rest modulo p, haves kongruenserne

$$hq \equiv \pm x \pmod{p}, \quad kp \equiv \mp x \pmod{q},$$

hvoraf følger, at samtlige tal α og β findes henholdsvis blandt tallene δ eller blandt tallene γ.

Angaaende postulatet om tallet c bemærker vi følgende: Er A og A' to hele tal, hvis sum er $\frac{1}{2}(q-1)p$, og sættes

(7) $$A \equiv -r \pmod{q}, \quad A' \equiv -r' \pmod{q},$$

haves bestandig

(8) $$r + r' \equiv \frac{p+q}{2} \pmod{q};$$

man finder nemlig efter en simpel omskrivning

$$A' = \frac{q-1}{2}p - A = \frac{p+1}{2}q - \frac{p+q}{2} - A \equiv$$
$$\equiv -\frac{p+q}{2} + r, \pmod{q},$$

og heraf kan (8) umiddelbart udledes.

Antager man dernæst, at A findes blandt tallene (3), vil det samme være tilfældet med A'; er endvidere $-r$ og $-r'$ numerisk mindste rester modulo q, findes ved (8)

(9) $$r + r' = \frac{p+q}{2},$$

hvoraf man slutter, at baade r og r' maa falde mellem $\frac{1}{2}p$ og $\frac{1}{2}q$. Disse rester r og r' forekommer derfor altid parvis, undtagen naar

$$p + q \equiv 0 \pmod 4, \tag{10}$$

hvor (9) kan tilfredsstilles af

$$r = r' = \frac{p+q}{4}. \tag{11}$$

Skal (11) kunne bestaa, haves tillige

$$A = A' = \frac{q-1}{4}p,$$

og q maa derfor være af formen $4k+1$, hvorefter (10) viser, at p maa være af formen $4h-1$; i dette og kun i dette tilfælde er c ulige.

Efter disse bemærkninger beviser man let følgende sætning:

II. *Tallene* $\lambda + \nu$ *og*

$$\omega = \frac{p-1}{2} \cdot \frac{q-1}{2} \tag{12}$$

er altid af samme paritet og er da og kun da ulige, naar q *er af formen* $4k-1$ *og* p *samtidig af formen* $4h-1$.

Der kan tænkes følgende fire muligheder:

1^0. $p=4h+1$, $q=4k\pm 1$, $\frac{1}{2}(p-1)=2h$, $\mu+\nu$ lige, ω lige
2^0. $p=4h-1$, $q=4k+1$, $\frac{1}{2}(p-1)=2h-1$, $\mu+\nu$ lige, ω lige
3^0. $p=4h-1$, $q=4k-1$, $\frac{1}{2}(p-1)=2h-1$, $\mu+\nu$ ulige, ω ulige.

Anvendes denne betragtning, erholdes ved formlen (5) den berømte reciprocitetssætning:

III. *Er* p *og* q *to ulige og forskellige primtal, haves stedse*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}. \tag{13}$$

Er derfor mindst et af primtallene p og q af formen $4n+1$, vil p være rest eller ikkerest modulo q, eftersom q er rest eller ikkerest modulo p. Er derimod baade p og q

af formen $4n - 1$, er p rest eller ikkerest modulo q, eftersom q er ikkerest eller rest modulo p.

Reciprocitetssætningen kendtes allerede, men sikkert uden bevis, af *Euler*[1]); *Legendre*[2]) har ikke haft held til at finde noget helt nøjagtigt bevis for sætningen; dette er først lykkedes *Gauss*[3]), som ialt har givet 8 beviser for den.

Reciprocitetssætningen har, lige siden *Gauss's* eksakte bevis, stadig interesseret talteoretikerne, og man kender nu et halvt hundrede mere eller mindre forskellige beviser[4]) for den; det ovenstaaende skyldes, med ringe modifikation, pastor *Christian Zeller*[5]).

Som eksempel vil vi søge de primtal, for hvilke tallene ± 3 er rester; af (13) findes

$$\left(\frac{3}{p}\right)\left(\frac{p}{3}\right) = (-1)^{\frac{p-1}{2}}. \tag{14}$$

Da nu ethvert primtal kan skrives paa en af formerne $12n \pm 1$ eller $12n \pm 5$, og da alle kvadrattal, som ikke er delelige med 3, modulo 3 giver resten 1, finder man

---

[1]) Opuscula analytica, Bd. I, p. 84. St. Petersborg 1783. Commentationes arithmeticæ collectæ, Bd. I, p. 487—506; St. Petersborg 1849.

[2]) Histoire de l'Académie (Paris) 1785, p. 465—559. (1788); se navnlig p. 516—517. Théorie des nombres, Bd. I, p. 230—243. Zahlentheorie. Bd. I, p. 229—242.

[3]) To beviser findes i Disquisitiones arithmeticæ, art. 135—145, art. 257—262. Untersuchungen über höhere Arithmetik, pp. 95—101, 273—283; Berlin 1889. Werke, Bd. I, pp. 104—111, 284—291. Tredje bevis findes i Commentationes Gottingenses, Bd. 16; 1808. Untersuchungen über höhere Arithmetik, p. 457—462. Werke, Bd. II, p. 1—8. Fjerde bevis i Commentationes Gottingenses recentiores, Bd. 1; 1811. Untersuchungen, p. 463—495 Werke, Bd. II, p. 9—45. Femte og sjette bevis i Commentationes Gottingenses recentiores, Bd. 4; 1818. Untersuchungen, p. 496—510. Werke, Bd. II, p. 47—64. Syvende og ottende bevis i Werke, Bd. II, p. 233—235.

[4]) *Otto Baumgart:* Ueber das quadratische Reziprozitätsgesetz; Leipzig 1885 *Bachmann*: Niedere Zahlentheorie, Bd. I, p. 180—318; Leipzig 1902. Sidstnævnte sted findes en tabellarisk oversigt over de forskellige beviser; se pp. 203—204, 402.

[5]) Berliner Monatsberichte, 1872, p. 846—847.

$$\left(\frac{12n \pm 1}{3}\right) = \pm 1, \quad \left(\frac{12n \pm 5}{3}\right) = \mp 1;$$

da man tillige henholdsvis har

$$\frac{p-1}{2} = 6n \text{ eller } 6n-1; \quad \frac{p-1}{2} = 6n+2 \text{ eller } 6n-3,$$

faas ved (14)

$$\left(\frac{3}{12n \pm 1}\right) = 1, \quad \left(\frac{3}{12n \pm 5}\right) = -1, \tag{15}$$

og altsaa erholdes sætningen:

IV. *Tallet* 3 *er rest for alle primtal af formen* $12n \pm 1$, *men ikkerest for alle primtal af formen* $12n \pm 5$.

Ifølge § 41, VI haves

$$\left(\frac{-1}{12n \pm 1}\right) = \pm 1, \quad \left(\frac{-1}{12n \pm 5}\right) = \pm 1;$$

hvoraf ved (15)

$$\left(\frac{-3}{12n \pm 1}\right) = \pm 1, \quad \left(\frac{-3}{12n \pm 5}\right) = \mp 1;$$

da nu endvidere

$$12n-5 = 6(2n-1)+1, \quad 12n+5 = 6(2n+1)-1,$$

haves:

V. *Tallet* -3 *er rest for alle primtal af formen* $6n+1$, *men ikkerest for alle primtal af formen* $6n-1$.

---

110. Antages a og b indbyrdes primiske, er tallet $a^2 + 3b^2$ ikke deleligt med noget primtal af formen $6n+5$.

KAPITEL XI.

Tals fremstilling ved kvadrattal.

§ 43. Algebraiske identiteter.

Cauchy[1]) har gjort opmærksom paa, at multiplikationsreglen for komplekse tal giver et simpelt middel til undersøgelse af produkter af faktorer, der alle er af en og samme specielle form.

Antages nemlig a, b, c og d reelle og α positiv, haves

$$(1)\quad (a + ib\sqrt{\alpha})\,(c + id\sqrt{\alpha}) = ac - bd\alpha + i\,(ad + bc)\sqrt{\alpha};$$

bemærkes det, at kvadraterne paa de ligestore absolute værdier af tallene i (1) er uafhængige af fortegnene for a, b, c, d, findes

$$(2)\quad (a^2 + b^2\alpha)\,(c^2 + d^2\alpha) = (ac \pm bd\alpha)^2 + (ad \mp bc)^2\,\alpha,$$

hvor tegnene paa højre side er sammenhørende.

Da (2) gælder for alle positive α, maa denne ligning være rigtig for alle mulige værdier af α, og altsaa findes sætningen:

I. *Produktet af et vilkaarligt antal faktorer, der alle er af formen* $a^2 + b^2\alpha$, *hvor* α *er et vilkaarligt helt tal, er paany et tal af samme form.*

Som det fremgaar af (2), kan det i I nævnte produkt i almindelighed paa flere maader bringes paa den omtalte form.

Vi fremhæver særlig de for $\alpha = \pm 1$ af I erholdte speciellere sætninger:

II. *Produktet af et vilkaarligt antal faktorer, som alle er en sum eller en differens af to kvadrattal, er selv henholdsvis en sum eller en differens af to kvadrattal.*

En sætning svarende til II om produkter af tal, som alle er en sum af tre kvadrattal, kan ikke gælde almindelig; man har nemlig f. eks.

---

[1]) Cours d'Analyse de l'Ecole Polytechnique, Bd. I, p. 181; Paris 1821.

$$(1+1+1)(16+4+1) = 63 = 8\cdot 7 + 7,$$

og et tal af formen $8n+7$ kan aldrig være en sum af tre kvadrattal.

Derimod har *Euler*[1]) af identiteten

$$(3)\quad \begin{cases} (a^2+b^2+c^2+d^2)(\alpha^2+\beta^2+\gamma^2+\delta^2) = \\ = (a\alpha+b\beta+c\gamma+d\delta)^2 + (a\beta-b\alpha-c\delta+d\gamma)^2 + \\ + (a\gamma+b\delta-c\alpha-d\beta)^2 + (a\delta-b\gamma+c\beta-d\alpha)^2, \end{cases}$$

der senere er generaliseret af *Lagrange*[2]), udledt sætningen:

III. *Produktet af et vilkaarligt antal faktorer, af hvilke hver enkelt er en sum af fire kvadrattal, er selv en sum af fire kvadrattal.*

V. A. Lebesgue[3]) har angivet en formel, hvoraf man specielt finder identiteten:

$$(4)\quad \begin{cases} (\alpha^2+\beta^2+\gamma^2+\delta^2)^2 = (\alpha^2+\beta^2-\gamma^2-\delta^2)^2 + \\ + (2\alpha\gamma+2\beta\delta)^2 + (2\alpha\delta-2\beta\gamma)^2, \end{cases}$$

hvoraf atter for $\delta = 0$

$$(5)\quad (\alpha^2+\beta^2+\gamma^2)^2 = (\alpha^2+\beta^2-\gamma^2)^2 + (2\alpha\gamma)^2 + (2\beta\gamma)^2,$$

og saaledes erholdes for $\alpha = 0$ eller $\beta = 0$ de *Pytagoræiske* tal.

Af (4) og (5) faas umiddelbart sætningen:

IV. *Kvadratet paa et tal, der skrives som en sum af tre eller fire kvadrattal, er altid en sum af tre kvadrattal.*

Graves[4]) og *Young*[5]) og lidt senere *Brioschi*[6]) har udvidet *Eulers* sætning III til at gælde for et produkt af faktorer, af hvilke hver enkelt er en sum af 8 kvadrattal, medens *S. Roberts*[7]) har forsøgt at bevise, at en lignende sætning

---

[1]) Commentationes arithmeticæ collectæ, Bd. I, p. 543. St. Petersborg 1849.
[2]) Mémoires de l'Académie de Berlin 1770, p. 133 (1772).
[3]) Comptes rendus, Bd. 66, p. 396—398; 1868.
[4]) I breve fra 1843 til *W. R. Hamilton*. Royal Irish Academy Proceedings, Bd. 3, p. 527—528; 1847. Transactions, Bd. 21 II, p. 338—340; 1848.
[5]) Philosophical Magazine 1845. Royal Irish Academy Proceedings, Bd. 3, p. 526—527; 1847. Transactions, Bd. 21 II, p. 311—338; 1848.
[6]) Crelles Journal, Bd. 52, p. 133—141; 1856.
[7]) Quarterly Journal of mathematics, Bd. 16, p. 159—170; 1879. Bd. 17, p. 276—280; 1880.

ikke gælder for produktet af faktorer, af hvilke hver enkelt er en sum af 2^n kvadrattal, hvor $n > 3$; men *Cayley* [1]) har gjort indvendinger mod dette bevis. Tidligere undersøgelser af denne art skyldes *Kirkman* [2]) og *Cayley* [3]); efter en paa grund af sin kortfattethed vanskelig forstaaelig note synes *Genocchi* [4]) at hævde muligheden af en yderligere udvidelse af *Eulers* sætning end den af *Graves*, *Young* og *Brioschi* givne.

Om *Eulers* og *Brioschis* sætninger haves endvidere et arbejde af *Buchta* [5]), hvis resultater i alt væsentlig synes at give *Roberts* uret.

Efter *Legendre* [6]) gør vi endnu her opmærksom paa identiteterne

$$(6) \qquad \begin{cases} 2(a^2 + b^2 + c^2) = (a + b)^2 + (a - b)^2 + 2c^2 \\ 2(a^2 + b^2 + 2c^2) = (a + b)^2 + (a - b)^2 + (2c)^2. \end{cases}$$

§ 44. **Sætninger af Fermat om fremstilling af visse primtal.**

Som et første eksempel paa talteoretiske anvendelser af de i foregaaende paragraf givne identiteter vil vi betragte kongruensen

$$(1) \qquad q^2 \equiv -\alpha \pmod{p},$$

hvor $\alpha = 1, 2, 3$, og hvor p er et saadant ulige primtal, at denne kongruens har løsninger.

Vi kan paa uendelig mange maader bestemme systemer af to hele tal x og y, af hvilke intet er deleligt med p, og saaledes at man har

$$(2) \qquad x + qy \equiv 0 \pmod{p},$$

og altsaa erholdes ved (1)

---

[1]) Quarterly Journal of mathematics, Bd. 17, p. 258—276; 1880.
[2]) Philosophical Magazine, Bd. 37, p. 294—295; 1850.
[3]) Philosophical Magazine (4) Bd. 4; p. 852.
[4]) Annali di mathematica, Bd. 3; 1860.
[5]) Sitzungsberichte der Wiener Akademie, Bd. 96, p. 110—133; 1887.
[6]) Théorie des nombres, Bd. I, p. 217. Zahlentheorie, Bd. I, p. 217.

$$x^2 + \alpha y^2 \equiv x^2 - q^2 y^2 \equiv 0 \pmod{p},$$

eller

$$x^2 + \alpha y^2 = pM, \tag{3}$$

hvor M er positiv hel.

Betegner i (3) x og y de modulo p numerisk mindste rester, haves $M < p$; ti $x^2 + \alpha y^2 < (1 + \alpha) p^2 : 4 \leqq p^2$, og dette gælder aabenbart for alle tre ovennævnte værdier $\alpha = 1$, $\alpha = 2$, $\alpha = 3$.

Vi skal nu bevise, at vi med (3) som udgangspunkt kan udlede en ligning af formen $p = x_1^2 + \alpha y_1^2$.

Lad os nemlig antage $M > 1$ og ved a og b betegne to vilkaarlige hele tal, da haves ifølge (3)

$$(x - aM)^2 + \alpha (y - bM)^2 = MM_1, \tag{4}$$

hvor M_1 er et nyt helt tal, som ikke kan være 0; ti antagelsen $M_1 = 0$ vilde medføre $x = aM$, $y = bM$, og altsaa fik man ved (3)

$$x^2 + \alpha y^2 = (a^2 + \alpha b^2) M^2 = pM, \quad (a^2 + \alpha b^2) M = p,$$

hvilket er umuligt, fordi p er et primtal, medens $M > 1$ og $a^2 + \alpha b^2 > 1$.

Antages i (4)

$$|x - aM| \leqq \tfrac{1}{2} M, \quad |y - bM| \leqq \tfrac{1}{2} M,$$

erholdes derfor $1 \leqq M_1 < M$; ti man ser af (3), at man ikke samtidig kan have

$$|x - aM| = \tfrac{1}{2} M, \quad |y - bM| = \tfrac{1}{2} M, \quad \alpha = 3,$$

og at disse forudsætninger er nødvendige for existensen af ligningen $M_1 = M$, er indlysende. Da M maa være lige, sætter vi $M = 2\mu$ og finder derved

$$x^2 = (2a \pm 1)^2 \mu^2, \quad y^2 = (2b \pm 1)^2 \mu^2,$$

hvorefter (3), idet $\alpha = 3$, giver

$$\mu ((2a \pm 1)^2 + 3 (2b \pm 1)^2) = 2p,$$

hvilket er umuligt, fordi venstre side er delelig med 4, medens højre side er af formen $4k + 2$.

Multipliceres dernæst (3) og (4), faas ved § 44, (2)

$$(x(x-aM)+\alpha y(y-bM))^2+\alpha(x(y-bM)-y(x-aM))^2=M^2M_1p$$
$$(x^2+\alpha y^2-(ax+\alpha by)M)^2+\alpha(ay-bx)^2M^2=M^2M_1p,$$

hvoraf under anvendelse af (3) og efter bortforkortning af M^2:

$$(5)\qquad (p-ax-\alpha by)^2+\alpha(ay-bx)^2=M_1p;$$

da $M_1<M<p$, kan intet af tallene paa venstre side i (5) være deleligt med p; ti saa maatte det andet ogsaa være det, og følgelig skulde $M_1p<p^2$ være deleligt med p^2.

Ligningen (5) er af samme form som (3), men $M_1<M$; havdes $M_1>1$, kunde man behandle (5) paa samme maade som før, o. s. v. Efter et endeligt antal transformationer af denne art erholdes derfor en fremstilling af formen

$$(6)\qquad x^2+\alpha y^2=p,$$

og vi skal nu bevise, at i denne ligning er tallene x og y entydig bestemte.

Havdes nemlig tillige følgende anden fremstilling af formen (6)

$$(7)\qquad x_1^2+\alpha y_1^2=p,$$

fik man ved multiplikation af (6) og (7)

$$(8)\qquad \begin{cases} p^2=(xx_1+\alpha yy_1)^2+\alpha(xy_1-x_1y)^2= \\ \quad =(xx_1-\alpha yy_1)^2+\alpha(xy_1+x_1y)^2, \end{cases}$$

og altsaa haves

$$(9)\qquad 0<|xy_1-x_1y|<p,\quad 0<|xx_1-\alpha yy_1|<p;$$

ti da x er primisk med y, og x_1 er primisk med y_1, medfører ligheden $xy_1=x_1y$, at $x=x_1$ og $y=y_1$. Havdes endvidere $xx_1=\alpha yy_1$, fik man $p^2=\alpha(xy_1+x_1y)^2$, hvilket ikke kan være muligt for $\alpha=2$, $\alpha=3$; for $\alpha=1$ giver den første $x=y_1$ og $x_1=y$, saa at i dette tilfælde (6) og (7) blev identiske.

Dernæst finder man ved (6) og (7)

$$p(y_1^2-y^2)=(x^2+\alpha y^2)y_1^2-(x_1^2+\alpha y_1^2)y^2=x^2y_1^2-x_1^2y^2,$$

Beviset for Fejlfeldes Lagrange, Nouveaux Mémoires de Berlin 1770, 123-133. Théorème de Fermat: Tout nombre est ou carré, ou composé de deux, ou de trois ou de quatre carrés.

og altsaa skulde p gaa op i et af tallene $xy_1 + x_1y$ eller $xy_1 - x_1y$, men dette er ifølge (9) ikke muligt.

Indføres nu efterhaanden de tre betragtede værdier $\alpha = 1$, $\alpha = 2$ og $\alpha = 3$, faas ved anvendelse af henholdsvis § 40, VI, § 41, IV og § 42, V følgende tre sætninger, som alle kendtes af *Fermat*[1]):

I. *Ethvert primtal af formen* $4n + 1$ *kan paa en og kun paa en maade skrives som en sum af to kvadrattal:* $p = x^2 + y^2$.

II. *Ethvert primtal af formen* $8n + 1$ *eller* $8n + 3$ *kan paa en og kun paa en maade skrives som en sum af et kvadrattal og det dobbelte af et kvadrattal:* $p = x^2 + 2y^2$.

III. *Ethvert primtal af formen* $6n + 1$ *kan paa en og kun paa en maade skrives som en sum af et kvadrattal og det tredobbelte af et kvadrattal:* $p = x^2 + 3y^2$.

Tillægger vi stedse α en af de tre ovennævnte værdier, ser vi, at en kongruens af formen

$$x^2 + \alpha y^2 \equiv 0 \pmod{p}, \tag{10}$$

hvor p er et primtal, x og y indbyrdes primiske, da og kun da er mulig, naar $-\alpha$ er en kvadratisk rest modulo p.

At ovennævnte betingelser er tilstrækkelige, ved vi af vore foregaaende undersøgelser. Da x og y er indbyrdes primiske ser vi straks, at hverken x eller y kan være delelig med p; det er derfor muligt at bestemme et saadant helt tal β, at

$$\beta y \equiv 1 \pmod{p}; \tag{11}$$

multipliceres dernæst i (10) med β^2 paa begge sider af kongruenstegnet, erholdes ifølge (11)

$$\beta^2 x^2 \equiv -\alpha\beta^2 y^2 \equiv -\alpha \pmod{p},$$

og altsaa er ovennævnte betingelse ligeledes nødvendig.

Af denne bemærkning faas umiddelbart sætningen:

IV. *Tillægger man* α *en af værdierne* 1, 2, 3, *og er* x *og* y *indbyrdes primiske, kan tal af formen* $x^2 + \alpha y^2$ *kun være delelige med ulige primtal, der selv er af samme form.*

---

[1]) Œuvres, Bd. II, pp. 212, 310, 402. Bd. III, p. 243.

En sum af to indbyrdes primiske kvadrattal kan saaledes ikke være delelig med noget primtal af formen $4n + 3$.

Da produktet af to tal af formen $x^2 + \alpha y^2$ paany er et tal af samme form, faas af (4) sætningen:

V. *Tillægger man* α *en af værdierne* 1, 2, 3, *maa enhver ulige divisor i et tal af formen* $x^2 + \alpha y^2$ *enten være et kvadrattal eller et tal af samme form.*

Ovenstaaende bevis skyldes *Legendre*[1]).

---

111. Bevis ved anvendelse af *Fermats* sætning § 29, I, at en sum af to indbyrdes primiske kvadrattal aldrig kan være delelig med et primtal af formen $4n + 3$.

112. Idet p er et primtal af formen $x^2 + \alpha y^2$, $\alpha = 1, 2, 3$, medens n er positiv hel, skal man bestemme antallet af maader, paa hvilke p^n kan fremstilles under denne form.

113. Vis, at ligningen $x^3 = y^2 + 17$ eller

$$(x + 2)((x - 1)^2 + 3) = y^2 + 5^2$$

ikke kan løses i hele tal[2]).

114. Vis, at $4n + 1 = x^2 + y^2$ da og kun da er mulig, naar n er en sum af to trigonaltal; n har altsaa altid denne egenskab, naar $4n + 1$ er et primtal[3]).

115. Undersøg de primtal, der kan fremstilles paa formerne $x^2 - 2y^2$ og $x^2 - 3y^2$.

§ 45. Lagranges bevis for Bachets sætning.

Som grundlag for vore undersøgelser af spørgsmaalet om, hvorvidt et vilkaarligt positivt helt tal kan skrives som en sum af kvadrattal, vil vi benytte følgende hjælpesætning, der i langt almindeligere form er given af *Lagrange*[4]):

---

[1]) Théorie des nombres, Bd. I, p. 203—204. Zahlentheorie, Bd. I, p. 203—205.

[2]) *Gérono* i Nouvelles Annales, (2) Bd. 16, p. 325—326; 1877.

[3]) *Euler* i Novi Commentarii Academiæ Petropolitanæ, Bd. 4, p. 26; 1752—53 (1758).

[4]) Mémoires de l'Académie de Berlin, 1770, p. 123—133; (1772).

Vis, at ethvert x bestemt ved $x^2 - 3y^2 = 1$ ikke kan indeholde andre ulige primfaktorer end saadanne af formen $3z^2 + 5^2$; vis dernæst, at samtlige A_{2n+1} er af formen $4k+2$.

Vis, at i ligningen $x^2 - 3y^2 = 1$ haves bestandig $A_{24} = 6A_{12}^2 + 1$.

Antages $x = 6z^2 + 1$, faas $12z^2(3z^2+1) = 3y^2$ altsaa $4z^2(3z^2+1) = y^2$, og følgelig haves $y = 2zu$, hvor $u^2 - 3z^2 = 1$. Da nu $B_{24} = 2A_{12}B_{12}$ faas $u = A_{12}$, $z = B_{12}$.

113. Tallet x kan ikke være lige; thi naar x er ulige, maa y være ulige, og $y^2 + 17$ følgelig et tal af formen $4n+2$, hvilket ikke kan være et kubiktal. Antages x ulige bliver $(x+1)^2 + 3$ et tal af formen $4n+3$, og dette tal kan ikke gaa op i $y^2 + 5^2$, naar y antages delelig med 5, $y = 5z$, eller $y^2 + 5^2 = 5^2(2^2+1)$.

Antages x ulige, medens alle primfaktorer i a er af formen $4n+1$, ses det, at ligningen

$$x^3 = y^2 + a^2 - (17)^3$$

ikke kan løses i hele tal.

I. *Det er muligt at bestemme fire positive hele tal a, b, c og d, der ikke alle er delelige med et og samme hele tal større end* 1, *og saaledes at*

$$a^2 + b^2 + c^2 + d^2 \equiv 0 \pmod{p}, \tag{1}$$

hvor p er et vilkaarligt primtal.

Lader man to af tallene a, b, c og d være lige, de to andre ulige, ser man straks, at sætningen gælder for primtallet 2. Er kun et af tallene a, b, c og d deleligt med 3, ser man ligeledes, at sætningen gælder for primtallet 3. Ved vort bevis kan vi derfor indskrænke os til kun at betragte et primtal $p = 2n + 1 \geqq 5$.

I dette øjemed vil vi ordne tallene fra 1 til $n - 1$ og fra $n + 1$ til $2n - 1$ parvis paa følgende maade

$$\begin{cases} 1 & 2 & 3 & \cdots\cdots & n-1 \\ 2n-1 & 2n-2 & 2n-3 & \cdots\cdots & n+1; \end{cases} \tag{2}$$

summen af tallene i hvert enkelt par er altsaa stedse $2n = p - 1$.

Da der blandt tallene fra 1 til $p - 1$ findes ialt $n = \frac{1}{2}(p - 1)$ kvadratiske rester modulo p, kan der tænkes følgende tre muligheder og ikke andre:

1 0. Hverken n eller $2n$ er kvadratiske rester modulo p. I dette tilfælde maa de $n - 1$ talpar (2) indeholde alle n kvadratiske rester, og mindst i et af disse par maa begge tallene derfor være kvadratiske rester. Er disse tal α og β, eksisterer der altsaa to positive hele tal a og b, saaledes at

$$a^2 \equiv \alpha \pmod{p}, \quad b^2 \equiv \beta \pmod{p},$$

og altsaa erholdes

$$a^2 + b^2 \equiv \alpha + \beta \equiv 2n \equiv p - 1 \equiv -1 \pmod{p};$$

i dette tilfælde finder man altsaa

$$a^2 + b^2 + 1 \equiv 0 \pmod{p}. \tag{3}$$

2 0. Er n kvadratisk rest modulo p, haves

$$a^2 \equiv n \pmod{p}, \quad 2a^2 \equiv 2n \equiv -1 \pmod{p},$$

og altsaa findes i dette tilfælde

(4) $$a^2 + a^2 + 1 \equiv 0 \pmod{p}.$$

3°. Er endelig $2n = p - 1$ en kvadratisk rest modulo p, haves

$$a^2 \equiv 2n \equiv -1 \pmod{p},$$

og altsaa er

(5) $$a^2 + 1 \equiv \pmod{p}.$$

Føjes nu til første led i kongruenserne (3) og (4) et vilkaarligt med p deleligt kvadrattal og til første led i (5) to saadanne, faas i alle tilfælde en kongruens af formen (1).

Ovenstaaende simple bevis skyldes *Matrot*[1]).

Vi vil dernæst bevise følgende sætning af *Lagrange*[2]):

II. *Ethvert primtal, som gaar op i en sum af fire kvadrattal, der ikke alle fire er delelige med samme hele tal større end* 1, *er selv en sum af højst fire kvadrattal.*

Er p et primtal, og haves

$$A^2 + B^2 + C^2 + D^2 \equiv 0 \pmod{p},$$

søger vi de numerisk mindste rester a, b, c, d modulo p af henholdsvis A, B, C, D; derved erholdes

(6) $$a^2 + b^2 + c^2 + d^2 = pp_1, \quad 1 \leqq p_1 < p.$$

Er $p_1 = 1$, har vi bevist vor sætning; er $p_1 > 1$, søger vi de numerisk mindste rester a_1, b_1, c_1, d_1 modulo p_1 af henholdsvis a, b, c, d, og finder altsaa ifølge (6)

(7) $$a_1^2 + b_1^2 + c_1^2 + d_1^2 = p_1 p_2, \quad 1 \leqq p_2 < p_1.$$

Man ser nemlig straks, at antagelsen $p_2 = 0$ er udelukket; ti ifølge vore forudsætninger kan ikke samtlige tal a, b, c og d være delelige med p_1. Antagelsen $p_2 = p_1$ medfører nødvendigvis p_1 lige, $p_1 = 2q$; ti i saa fald kan intet af tallene a_1, b_1, c_1 og d_1 være numerisk mindre end $\frac{1}{2}p_1$; endvidere haves

---

[1]) Association française pour l'avancement des Sciences. Congrès à Limoges 1890, p. 79–81.

[2]) Mémoires de l'Academie de Berlin 1770, p. 126 (1772).

$$a^2 = (2\alpha \pm 1)^2 q^2, \quad b^2 = (2\beta \pm 1)^2 q^2,$$
$$c^2 = (2\gamma \pm 1)^2 q^2, \quad d^2 = (2\delta \pm 1)^2 q^2,$$

hvilket ifølge (6) er umuligt.

Ved multiplikation af (6) og (7) faas dernæst under anvendelse af § 43, (3) en ligning af formen

$$\alpha^2 + \beta^2 + \gamma^2 + \delta^2 = pp_1^2 p_2, \tag{8}$$

hvor vi for kortheds skyld har sat

$$\begin{cases} \alpha = aa_1 + bb_1 + cc_1 + dd_1 \\ \beta = ab_1 - ba_1 - cd_1 + dc_1 \\ \gamma = ac_1 + bd_1 - ca_1 - db_1 \\ \delta = ad_1 - bc_1 + cb_1 - da_1 \end{cases} \tag{9}$$

Af definitionerne for a_1, b_1, c_1, d_1 faas ligninger af formen

$$a_1 = a - k_1 p, \quad b_1 = b - k_2 p_1, \quad c_1 = c - k_3 p, \quad d_1 = d - k_4 p,$$

hvor k_1, k_2, k_3, k_4 er hele tal; indføres disse udtryk i (9), og anvendes (6), ses det, at alle fire tal α, β, γ, δ bliver delelige med p_1. Bortforkortes derefter p_1^2 af (8), faas en ny ligning af samme form som (6)

$$a_2^2 + b_2^2 + c_2^2 + d_2^2 = pp_2. \tag{10}$$

Er her $p_2 = 1$, giver (10) den søgte sætning; er $p_2 > 1$, behandles (10) paa samme maade som (6), o. s. v. Da $p_2 < p_1$, o. s. v., maa vi ved denne fremgangsmaade engang komme til en ligning af formen

$$a_m^2 + b_m^2 + c_m^2 + d_m^2 = p. \tag{11}$$

Af I og II faas derefter umiddelbart sætningen:

III. *Ethvert primtal er en sum af højst fire kvadrattal.*

Anvendes endelig den *Eulerske* sætning § 43, III, faas almindelig:

IV. *Ethvert positivt helt tal er en sum af højst fire kvadrattal.*

Denne sætning tilskrives sædvanlig *Bachet*[1]); men hverken han eller *Euler*[2]) har kunnet give noget bevis for den; dette er først lykkedes *Lagrange*; men det bør dog bemærkes, at *Euler*[3]) senere betydelig simplificerede det af *Lagrange* givne bevis.

Er n et vilkaarligt helt tal, og sættes

$$n = a^2 + b^2 + c^2 + d^2,$$

findes ved § 43, (4) sætningen:

V. *Ethvert kvadrattal er en sum af højst tre kvadrattal.*

Vi kan ikke her behandle andre fremstillingsformer af hele tal ved hjælp af kvadrattal; vi skal endnu blot nævne, at *Fermat*[4]) har fremsat den sætning, at ethvert positivt helt tal kan skrives som en sum af højst n n-kantstal.

For $n = 4$ faas altsaa specielt *Bachets* sætning; for $n = 3$, at ethvert helt tal kan skrives som en sum af højst 3 trigonaltal.

Denne mærkelige sætning af *Fermat* er bevist af *Legendre*[5]).

---

[1]) *Wertheim*: Die Arithmetik und die Schrift über Polygonalzahlen des Diophantus von Alexandria, p. 162; Leipzig 1890. *Bachet* har fremstillet de positive hele tal indtil 325 som summer af kvadrattal.

[2]) *Wertheim*: Anfangsgründe der Zahlenlehre, p. 393; Braunschweig 1902.

[3]) Acta Academiæ Petropolitanæ 1777, II, p. 48—69; 1780.

[4]) Œuvres, Bd. II, p. 63.

[5]) Théorie des nombres, Bd. II, p. 340—354. Zahlentheorie, Bd. II, p. 332—348. Sammenlign *Gauss*: Disquisitiones arithmeticæ, art. 293. Arithmetische Untersuchungen, p. 334; Berlin 1889. Werke, Bd. I, p. 348—349.

INDHOLDSFORTEGNELSE.

KAPITEL I.

Om division.

§ 1. Divisionsrester. Opg. 1—5 1
§ 2. Den Euklidiske algoritme. Opg. 6 5
§ 3. Største fælles faktor og mindste fælles multiplum. Opg. 7—11 . 6
§ 4. Ubestemte ligninger af første grad med to ubekendte. Opg. 12—13 9
§ 5. Kongruenser. Opg. 14—15 11
§ 6. Talsystemer. Opg. 16—17 14

KAPITEL II.

Primtal.

§ 7. Sætninger om primtal. Opg. 18—24 17
§ 8. Om mængden af primtal. Faktortavler. Opg. 25 19
§ 9. Eratostenes's sigte. Legendres regel. Opg. 26—27 23

KAPITEL III.

Sammensatte tal.

§ 10. Antal og sum af et tals divisorer Opg. 28—31. 24
§ 11. Den Eulerske funktion $\varphi(n)$. Opg. 32—35 27
§ 12. Opløsning i primfaktorer af $n!$ Opg. 36—40. 29

KAPITEL IV.

Fuldkomne og venskabelige tal.

§ 13. Sætninger om fuldkomne tal. Opg. 41—42 32
§ 14. Legendres undersøgelser over venskabelige tal 36
§ 15. Eulers og Seelhoffs undersøgelser over venskabelige tal 38

KAPITEL V.

Talteoretiske funktioner.

§ 16. Eksempler. Potenssummer og fakultetkoefficienter. Opg. 43—47 39
§ 17. Differensrækker af vilkaarlig orden. Opg. 48 43
§ 18. Undersøgelse af potenssummerne $S_p(n)$. Opg. 49—56 46
§ 19. Videre undersøgelse af polynomiet $\Phi_p(x)$. Opg. 57—61 51
§ 20. Nikomakos's regel. Liouvilles sætning. Opg. 62—66 56
§ 21. Tal af specielle former. Opg. 67—69 58

KAPITEL VI.

Fermats problem.

§ 22. Bemærkninger om kædebrøker. Opg. 70 - 72 61
§ 23. Lagranges sætning om periodiske kædebrøker. Opg. 73—74 . . 66
§ 24. Rent kvadratiske ligninger 70
§ 25. Lagranges løsning af Fermats problem. Opg. 75—84 75

KAPITEL VII.

Kvadrattal og bikvadrattal.

§ 26. Pytagoræiske tal. Opg. 85—87 81
§ 27. Fermats og Eulers sætninger om bikvadrater. Opg. 88 84
§ 28. Andre anvendelser af de Pytagoræiske tal. Opg. 89—92. . . . 88

KAPITEL VIII.

Fermats og Wilsons sætninger.

§ 29. Eulers generalisation af Fermats sætning. Opg. 93—94 91
§ 30. Dirichlets bevis for Fermats sætning 93
§ 31. Gauss's generalisation af Wilsons sætning. Opg. 95—96 95
§ 32. Lagranges bevis for Fermats og Wilsons sætninger. Opg. 97—98 98
§ 33. Fermats og Mersennes tal 99

KAPITEL IX.

Kongruenser for primtalmodulus.

§ 34. Algebraiske kongruenser. Lagranges sætning. Opg. 99—101. . 104
§ 35. Fermats kongruens. Opg. 102—103 108
§ 36. Gauss's teori om tals indeks 111
§ 37. Perioder hørende til et tal 114
§ 38. Primitive rødder i Fermats kongruens 115
§ 39. Den almindelige binome kongruens. Opg. 104 120

KAPITEL X.

Kvadratiske rester.

§ 40. Eulers kriterium. Legendres symbol. Opg. 105—108 121
§ 41. Gauss's lemma. Opg. 109 124
§ 42. Reciprocitetssætningen for kvadratiske rester. Opg. 110 127

KAPITEL XI.

Tals fremstilling ved kvadrattal.

§ 43. Algebraiske identiteter 132
§ 44. Sætninger af Fermat om fremstilling af visse primtal. Opg. 111—115 134
§ 45. Lagranges bevis for Bachets sætning 138